Chat criptate e diritto processuale penale

di Fabio Di Vizio*[1]

SOMMARIO: -1. Introduzione. - 2. Il funzionamento dei sistemi SkyEcc e Encrochat e le indagini "a monte" delle autorità straniere. - 3. I temi in campo: lo strumento processuale "interno" per importare le "chat" decrittate oggetto dell'OEI, la competenza ad autorizzare l'attività di indagine e ad avanzare la richiesta di cooperazione sino all'ambito del controllo giurisdizionale interno. - 3.1. Il protocollo dell'art. 234-*bis* c.p.p. ed i corollari. – 3.2. Le critiche al protocollo dell'art. 234-*bis* c.p.p. e il favore per l'inquadramento nell'art. 254-*bis* c.p.p., con le conseguenze. – 3.3. L'acquisizione come documenti *ex* art. 234 c.p.p. - 3.4. L'acquisizione quale attività di intercettazione. - 3.5. L'acquisizione dei risultati delle intercettazioni eseguite da autorità straniera, la verifica del rispetto delle condizioni *ex* artt. 270 e 271 c.p.p. e i corollari. – 4. Garanzie difensive interne per l'importazione delle comunicazioni decrittate nel procedimento estero e acquisite a seguito di OEI. - 4.1. I principi di proporzionalità e di equivalenza secondo l'ordinamento interno: le attività di indagine governate da tali regole. - 4.2. Il principio di equivalenza e la legittimità della decriptazione realizzata captando chiavi crittografiche. - 4.3. Il contraddittorio sul processo di formazione della prova e il diritto della difesa di accesso all'algoritmo di decriptazione e agli originali messaggi criptati. – 5. Il quadro giurisprudenziale delle Corti europee e le prospettive future.

1. Introduzione.

L'**evoluzione tecnologica** origina continue tensioni nei diversi settori del diritto, sottoponendoli a "**stress da modernità**". In generale, oggettiva è la difficoltà dell'ordinamento di adeguare le sperimentate **categorie giuridiche** agli innovativi schemi di realizzazione delle condotte umane, le quali si giovano di originali **infrastrutture informatiche e telematiche** combinate con sempre più evoluti **modelli statistici**. Inoltre, non è inconsueta una certa resistenza degli interpreti a cogliere il cambiamento, per una naturale tendenza a (voler) decriptare la realtà secondo la bussola rassicurante dell'esperienza. Questa impostazione può esporre al rischio di sottovalutare le differenze originali dei diversi meccanismi sottesi alle novità tecnologiche anche quando consistenti e suscettibili di alterare le conclusioni giuridiche raggiunte. **Conoscere la tecnica moderna** – componente ormai consustanziale del fatto umano - è divenuta condizione irrinunciabile del **buon diritto**.

Il diritto processuale penale – in particolare la disciplina dei mezzi di ricerca della prova - costituisce settore nel quale tali difficoltà di adattamento si registrano con maggiore evidenza. La circostanza è significativa. Nell'ambito della prova scientifica - di cui quella tecnologica è specificazione - va censita, infatti, la tendenza ad una **generale anticipazione alla fase delle indagini delle garanzie e del metodo del contraddittorio**, assumendone tardiva l'attivazione solo dopo l'apertura del dibattimento[2]. Così il giurista e l'operatore del diritto si trovano non solo a riconoscere ma addirittura ad amministrare una generale retrocessione delle garanzie di partecipazione della formazione della prova, "dal processo all'indagine"; linea evolutiva, invero, accentuata anche dalla più estesa giurisdizionalizzazione di quest'ultima avuta di mira da recenti riforme (d.lgs. n. 150/2022,

[1] Sostituto Procuratore presso la Direzione Distrettuale antimafia della Procura di Firenze.

[2] Come annota M. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in Giurisprudenza Penale Web, 2023, 10, 25, il contraddittorio non verte solo sull'oggetto da provare, bensì anche su tutte le attività intese a farlo. Perciò, «ogni forma di contraddittorio presuppone una dualità antagonistica e paritetica, nel senso che i suoi protagonisti debbono essere portatori di interessi e obbiettivi diversi, anche se nella disputa possono trovare uno o più punti di convergenza, e debbono godere di equivalenti diritti. Primo fra tutti, tanto da doverlo considerare un presupposto di esistenza del contraddittorio, quello di **conoscere compiutamente l'oggetto del contendere** (G. CONSO, *Considerazioni in tema di contraddittorio nel processo penale italiano*, in *Riv. it. dir. e proc. pen*., 1966, p. 405 ss.). Il principio del contraddittorio va inteso quale *work in progress*, che si snoda lungo una sequela di atti, che dalla domanda (imputazione), necessaria per porre il tema della contesa, trova nella sentenza lo strumento che la risolve (F. CORDERO, *Riti e sapienza del diritto*, Bari, 1981, p. 433).

cd. Cartabia). Un governo affidato a strumenti con potenzialità e limiti di impiego che scontano, però, non pochi difetti di determinatezza.

Un deciso orientamento può attendersi dalla considerazione della **scala di valori in campo**, ma la stessa non risulterà mai completamente risolutiva, potendo reggersi su **bilanciamenti mutevoli**: gli interessi, infatti, possono risultare divergenti quand'anche parimenti degni. Si pensi, da una lato, al potenziamento della cooperazione giudiziaria ed interforze tra gli Stati dell'Unione europea, che ormai travalica la semplice assistenza, secondo un'evoluzione necessitata dall'emergere di nuove forme di criminalità transnazionale e dall'esigenza di assicurare la ricerca della verità, declinata nel "necessario accertamento dei fatti aventi rilevanza penale"[3] e dunque nel dovere "di conservazione e non dispersione degli elementi di prova legittimamente acquisiti"[4]; si consideri, d'altro canto, la necessità di riconoscere e strutturare uno *ius commune* per la salvaguardia dei diritti fondamentali, capace di evitare letture esegetiche funzionalizzate esclusivamente alla ricerca della verità da assicurare "ad ogni costo", anche al prezzo di abdicare alle garanzie di un equo e sereno processo degli indagati-imputati.

Negli ultimi anni il diritto processuale penale ha registrato, in effetti, una pervasiva rilettura degli strumenti di indagine e dei mezzi di contrasto patrimoniale dei proventi illeciti alla luce dei **principi di proporzionalità e di adeguatezza**; principi sempre più cosmopoliti e interdisciplinari, che trovano innovative declinazioni in quasi tutti i campi del diritto, sotto diversi nomi; siano essi la ragionevolezza, la razionalità, l'equità, l'esigibilità, l'equilibrio tra interessi, l'efficacia e l'efficienza dello strumento rispetto agli obiettivi. Proporzionalità che dalla fase preventiva (si pensi al *risk-based approach*) si trasferisce anche a quella del controllo e dell'accertamento delle responsabilità[5]. Ciò avviene nel contesto di una visione dinamica del rapporto tra i diritti fondamentali dell'individuo e le esigenze pubbliche di sicurezza e benessere, senza precostituite prevalenze delle seconde sui primi. Quella in analisi costituisce una prospettiva irrinunciabile, potrebbe dirsi identitaria dei principi dell'ordinamento costituzionale interno, convenzionale ed unionale, sempre più nitida anche nella trama delle pronunce delle alte Corti nazionali e sovranazionali, che stanno forgiando per via giudiziale **nuovi statuti della prova tecnologica**[6].

Non vanno taciute le problematiche, oggettivamente grandi, che l'irrompere dell'adeguatezza e della proporzionalità negli strumenti di indagine e nella risposta ripristinatoria e sanzionatoria pone al magistrato inquirente e al giudice, con soluzioni concrete difficilmente predeterminabili; esse arrivano ad implicare anche inconsuete **rinunce o autolimitazioni secondo il perimetro della fattispecie concreta**, oltre che quello della norma astratta[7]. Sotto il primo profilo, ad esempio, è stato precisato come «la portata precettiva degli artt. 42 Cost. e 1 del primo Protocollo addizionale della

[3] Corte cost., 26 marzo 1993, n. 111, in www.cortecostituzionale.it.

[4] Corte cost., 2 novembre 1998, n. 361, in www.cortecostituzionale.it.

[5] Nella relazione illustrativa del d.lgs. n. 108 del 2017 si afferma, in ordine al necessario rispetto del principio di proporzionalità alla base sia dell'emissione che dell'esecuzione dell'OEI (Cass. Sez. VI, n. 8320 del 31/01/2019, Creo, cit.), che all'autorità giudiziaria è affidato il vaglio circa «...la capacità **del mezzo richiesto di raggiungere l'obiettivo prefissato, secondo il criterio per il quale, a parità di efficacia, è da preferire sempre il mezzo che abbia conseguenze meno gravose**. La proporzionalità adeguatezza impone di porre in bilanciamento, da un lato, la restrizione imposta al singolo e, dall'altro, il valore del fine perseguito dal pubblico potere nell'esercizio della funzione. In questa valutazione, **l'interprete sarà necessariamente guidato dalla natura del fatto per cui si procede**».

[6] G. SPANGHER, *Servono regole di garanzia per la prova informatica,* in Penale Diritto e Procedura, 2/2023, pp. 425-428.

[7] Deve intercorrere un nesso funzionale tra ogni singolo bene appreso - quand'anche corpo di reato - e l'accertamento del fatto, nel rispetto dei principi di proporzionalità, adeguatezza e gradualità, secondo l'insegnamento della giurisprudenza europea rispetto al bilanciamento tra i diversi interessi in gioco e il sacrificio del diritto di proprietà (Corte Edu, 13 ottobre 2015, Unsped Paket Servisi, SaN. Ve TiC. A.Åž. c. Bulgaria; Corte Edu 13 dicembre 2016, S.C. Fiercolect Impex S.R.L. c. Romania) evitando limitazioni alla proprietà privata non strettamente conseguenti alla finalità istituzionalmente perseguita dalla misura probatoria (Cass., SU, 36072 del 19/04/2018, Botticelli, Rv. 273548); il decreto di sequestro probatorio, anche se ha ad oggetto cose costituenti corpo del reato, deve contenere una specifica motivazione della finalità perseguita per l'accertamento dei fatti. Parimenti è a dirsi per le cose pertinenti al reato, nozione che evidentemente segnala una relazione meno immediata ma pur sempre funzionale rispetto al reato.

Convenzione Edu richiede che le **ragioni probatorie** del vincolo di temporanea indisponibilità della cosa, anche quando la stessa si identifichi nel corpo del reato, siano esplicitate nel provvedimento giudiziario con adeguata motivazione, allo scopo di garantire che la misura, a fronte delle contestazioni difensive, sia soggetta al permanente controllo di legalità - anche sotto il profilo procedimentale - e di concreta idoneità in ordine all'*an* e alla sua durata, in particolare per l'aspetto del giusto equilibrio o del ragionevole rapporto di **proporzionalità tra il mezzo impiegato, ovvero lo spossessamento del bene, e il fine endoprocessuale perseguito**, ovvero l'accertamento del fatto di reato (Corte Edu, 24 ottobre 1986, Agosi c. U.K.). Ed ogni misura, per dirsi proporzionata all'obiettivo da perseguire, dovrebbe richiedere che ogni interferenza con il pacifico godimento dei beni trovi un giusto equilibrio tra i divergenti interessi in gioco (Corte Edu 13 ottobre 2015, Unsped Paket Servisi SaN. Ve TIC. A. S. c. Bulgaria)»[8].

Un'autorità giudiziaria – quella giudicante - chiamata, problematicamente, a non applicare sanzioni sproporzionate al fatto per la punizione già inflitta[9] o - quella requirente, *in primis* - a **limitare rigorosamente le esigenze investigative nel tempo e per gli oggetti concretamente vincolabili** si trova responsabilizzata nell'esercizio innovativo di poteri tradizionali. In questa nuova prospettiva, senza arrivare a sostenere che il giudice non è più richiesto di applicare la legge ma di declinarla, è giusto riconoscere che ciò implica la **ridefinizione della regola alla luce del fatto da accertare**, segnando **per via giudiziale** i confini concreti degli interessi in gioco. Così, in concomitanza con l'estensione della nozione tradizionale di "legge", la sostanza della regola si avvicina al fatto concreto, trovando nel giudice uno dei suoi artefici. Uno sviluppo che può apparire disorientante per la cultura di *civil law* e che si pone all'origine di continui turbamenti ordinamentali nel contesto dell'assetto costituzionale.

È nota l'ulteriore preoccupazione sottesa a questa evoluzione. Per via della torsione del metodo ermeneutico o del potenziale sconfinamento istituzionale, dal congiunto operare della dimensione giurisprudenziale del "diritto vivente" e del principio di legalità formale sorge il **pericolo di un affievolimento delle garanzie di conoscibilità del comando e di prevedibilità, stabilità e uniformità della decisione, con declino della certezza del diritto**. Molta fiducia viene riposta nella **capacità nomofilattica della Cassazione**. E puntualmente si è notato che la nomofilachia non è statica conservazione di orientamenti giurisprudenziali cristallizzati nel tempo, ma «capacità di adeguare l'interpretazione delle norme al continuo mutare delle esigenze e dei costumi, entro i confini consentiti e alla luce dei principi posti dalla Costituzione, in modo il più possibile ordinato e coerente, così da rendere chiari i criteri di fondo cui il diritto vivente s'ispira, in un fecondo dialogo con lo stesso Legislatore»[10]. Nell'esperienza comune, però la **capacità equilibratrice della Cassazione** vive **serie difficoltà**. In questo contesto, problematico quanto complesso, la predeterminazione del precetto, anche di quello che funziona quale regola di comportamento nella ricerca degli elementi di prova, si fa più evanescente, richiedendo una sensibilità nuova quanto necessaria nell'equilibrio tra garanzie dell'individuo ed esigenze dello Stato. È questa complessità figlia di una condizione del rapporto con la legge ed i principi del diritto diversi dalla tradizione nazionale e da quel che deriva

[8] Cass., SU, n. 36072/2018, cit.

[9] Cfr. C. cost. n. 112/2019 ha dichiarato l'illegittimità costituzionale dell'art. 187-*sexies* TUF, nel testo originariamente introdotto dall'art. 9, comma 2, lettera a), della legge n. 62 del 2005, nella parte in cui prevede la confisca obbligatoria, diretta o per equivalente, del «prodotto» dell'illecito e dei «beni utilizzati» per commetterlo, e non del solo «profitto». Si veda anche Cass., Sezione tributaria, 27564/2018 in tema della verifica da parte del giudice della proporzionalità ed afflittività complessiva delle sanzioni penali ed amministrative unitariamente considerate.

[10] Annota G. CANZIO, *Cassazione e legalità penale*, Parma 9-10 ottobre 2015, reperibile in *https://romatrepress.uniroma3.it/wp-content/uploads/2019/05/6cass-gica.pdf*: «Essa non è un valore assoluto ma metodologico e, nell'inarrestabile evoluzione della giurisprudenza, confluisce dinamicamente nel «dovere funzionale di ragionevole mantenimento della soluzione ragionevolmente conseguita» (G. Borrè). Il reciproco e virtuoso esercizio dell'*ars legiferandi* e dell'*ars interpretandi* trova così un solido punto di equilibrio nel ruolo e nella funzione nomofilattica della Corte di Cassazione (F. Palazzo), al cui magistero è affidato il compito di depotenziare il corto circuito fra la legalità formale della legge e la legalità effettuale della giurisprudenza».

dall'esperienza del diritto comunitario, prima, ed eurounitario, poi, nella mediazione interpretativa offerta dalle Alte Corti europee. Ed è difficoltà resa evidente dal fatto che le contrapposizioni si formano in seno alle stesse comunità di professionisti del diritto - alle stesse Sezioni della Cassazione - e conducono in breve a reiterate richieste di interventi dell'organo supremo di nomofilachia.

Miope risulterebbe qualsiasi pretesa di **uscire da questo stato di insicurezze con "certezze forzate"**; si richiamino a **presunzioni o predefinizioni di esiti scientifici** ricevuti ma non sperimentati e ripercorsi in termini logico-razionali. Una **resistenza al dubbio che può essere solo temporanea** e non vi porrà argine. Le garanzie sui cui si edifica il diritto penale ed in funzione delle quali si struttura la procedura esigono **ragionevoli certezze -** e non semplici presunzioni - **di osservanza**.

L'**acquisizione da ordinamenti stranieri e l'utilizzazione nelle indagini interne della cd. chat decriptate** rappresenta un'**evenienza paradigmatica** delle problematicità che si sono venute esponendo ora in termini generali.

All'origine dell'insorgere delle più intense diversità di vedute sulle **modalità di acquisizioni delle chat e sui controlli** rispetto ad esse instaurabili, il significativo mutamento dell'interpretazione giurisprudenziale offerta alla **nozione di corrispondenza e di comunicazione informatica**. La Corte costituzionale, con la sentenza n. 170 del 27 luglio 2023, ha riconosciuto che la posta elettronica e i messaggi inviati tramite l'applicazione WhatsApp, anche se già letti[11], sono equiparati a lettere o biglietti chiusi e, rientrando nella sfera di protezione dell'art. 15 Cost., sono sottoposti alla duplice garanzia della riserva di legge e di giurisdizione[12]. Secondo il Giudice delle Leggi la tutela dei precetti costituzionali non si esaurisce con la ricezione del messaggio da parte del destinatario, ma perdura fin tanto che per gli interlocutori si mantenga un interesse attuale alla loro salvaguardia. Il concetto di «corrispondenza» ricomprende, perciò, ogni comunicazione di pensiero umano tra due o più persone determinate e si attua anche in modo diverso dalla conversazione *in itinere*. Se la nozione di comunicazione, poi, non è incisa né dalla materia o dall'oggetto in cui si concreta il contenuto della stessa, né dalla forma espressiva adoperata per trasmettere il pensiero (ad es. la lingua o segni), né dal mezzo (gli ordinari servizi postali e di telecomunicazione, nonché altri mezzi particolari) di trasmissione del contenuto della comunicazione, a circoscrivere l'ambito di tutela dell'art. 15 Cost. restano il carattere necessariamente inter-subiettivo o personale della comunicazione o della corrispondenza (dovendo essere formulate da un mittente e fatte pervenire nella sfera di conoscenza di uno o più destinatari) e il carattere dell'«attualità», che verrà meno «quando, ormai, per il decorso

[11] Ai fini della risoluzione del quesito, la Corte costituzionale ha esaminato le ricostruzioni già riconosciute. Secondo un primo, più garantista, indirizzo interpretativo, "la tutela – iniziata nel momento in cui l'espressione del pensiero è affidata ad un mezzo idoneo a trasmetterlo, rendendo così fattivo l'intento di comunicarlo ad altri – non si esaurirebbe con la ricezione del messaggio e la presa di cognizione del suo contenuto da parte del destinatario, ma permarrebbe finché la comunicazione conservi carattere di attualità e interesse per i corrispondenti. Essa verrebbe meno, quindi, solo quando il decorso del tempo o altra causa abbia trasformato il messaggio in un documento "storico", cui può attribuirsi esclusivamente un valore retrospettivo, affettivo, collezionistico, artistico, scientifico o probatorio". Secondo altro indirizzo interpretativo, più riduttivo, invece, "la corrispondenza già ricevuta e letta dal destinatario non sarebbe più un mezzo di comunicazione, ma un semplice documento". La garanzia apprestata dall'art. 15 Cost. si giustificherebbe, infatti, con la particolare "vulnerabilità" dei messaggi nel momento in cui sono "corrisposti", per "il maggior rischio di captazione o apprensione da parte di terzi: essa cesserebbe, quindi, con l'esaurimento dell'atto del corrispondere, coincidente con il momento in cui il destinatario prende cognizione della comunicazione. Dopo tale momento, la corrispondenza resterebbe tutelata, non più dall'art. 15 Cost., ma da altre disposizioni costituzionali, quali quelle in materia di libertà personale e domiciliare, libertà di manifestazione del pensiero, diritto di difesa o diritto di proprietà". Tra le due opposte tesi, la Consulta ha preferito la prima tesi, sostenuta dal Senato della Repubblica, osservando che "degradare la comunicazione a mero documento quando non più in itinere, è soluzione che, se confina in ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, sempre più ridotti, di corrispondenza cartacea, finisce addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione".

[12] Per un commento, M. BORGOBELLO, *Il concetto di corrispondenza nella sentenza 170 del 2023 della Corte costituzionale*, in *Giur. Pen. web,* n. 8, 2023.

del tempo o per altra causa non gli si può assegnare (alla comunicazione o alla corrispondenza) che un valore meramente retrospettivo, affettivo, collezionistico, storico, artistico, scientifico o probativo»[13]. Nondimeno, la Corte costituzionale ha ammesso la prerogativa parlamentare prevista dall'art. 68, terzo comma, Cost. anche per i tabulati telefonici (sentenza n. 38 del 2019)[14]. Ma se, dunque, l'acquisizione dei dati esteriori di comunicazioni già avvenute (quali quelli memorizzati in un tabulato) gode delle tutele accordate dagli artt. 15 e 68, terzo comma, Cost., è ritenuto impensabile che non ne fruisca, invece, il sequestro di messaggi elettronici, anche se già recapitati al destinatario: operazione che consente di venire a conoscenza non soltanto dei dati identificativi estrinseci delle comunicazioni, ma anche del loro contenuto, e dunque di attitudine intrusiva tendenzialmente maggiore.

Tale approdo della Corte costituzionale ha avuto almeno due riflessi sulla materia che interessa. Anzitutto, ha fatto emergere **dubbi sulla natura documentale-informatica attribuita alla messaggistica SkyEcc** dall'impostazione esegetica dominante. Inoltre, ha condotto ad interrogarsi se da questa nuova lettura scaturiscano riflessi sul **modulo di ricerca della prova attivabile nel contesto della cooperazione giudiziaria unionale** (in particolare tenuto conto della direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014), conducendo a ritenere non più sufficiente la semplice **importazione di documenti già acquisiti** alla disponibilità dell'autorità estera *ex* art. 45 d.lgs. n. 108/2017 ma necessario lo **svolgimento di attività di indagine su iniziativa dell'A.G. requirente** *ex* art. 43 d.lgs. n. 108/2017, con **preventive autorizzazioni dell'A.G. giudicante per l'attività di intercettazion**e. Dubbio che attiene ai possibili **termini del controllo, preventivo o successivo**, che rispetto a tale acquisizione probatoria deve o comunque può essere chiamato a svolgere il **giudice nazionale**.

Contrasti sempre maggiori, cui sembrano seguire **certezze diverse ed in evoluzione**. Così nella ordinanza di rimessione alle Sezioni Unite la Cass., Sez. III, 47798/2023 ha osservato la possibilità di un contrasto giurisprudenziale in ordine alle seguenti questioni: «a) Se in tema di mezzi di prova l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante O.E.I., presso A.G. straniera che ne ha eseguito la decrittazione, costituisca **acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* cod. proc. pen.** a mente del quale "è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare" **o di documenti *ex* art. 234 cod. proc. pen. o sia riconducibile in altra disciplina** relativa all'acquisizione di prove; b) Se inoltre, tale acquisizione debba essere oggetto, ai fini della **utilizzabilità** dei dati in tal modo versati in atti, di **preventiva o successiva verifica giurisdizionale della sua legittimità da parte della Autorità giurisdizionale nazionale**». Nel breve volgere di qualche mese, prima ancora dell'intervento delle Sezioni Unite, la Sesta Sezione della Cassazione (sent. n. 2329/2024) ha ritenuto di poter escludere - quanto all'individuazione del corretto strumento processuale "interno" da porre a parametro per l'importazione delle "chat" decrittate e richieste con gli OEI - uno dei termini dell'alternativa introdotta dalla Terza Sezione (lo strumento processuale di cui all'art. 234-*bis* c.p.p. soluzione, invero sin qui ampiamente preferito nell'esperienza delle pronunce del giudice di legittimità) limitando le alternative al sequestro di corrispondenza informatica *ex* art. 254-*bi*s c.p.p. o all'acquisizione di risultanze delle intercettazioni acquisite *ex* art. 270 c.p.p.; nella stessa occasione, la Sesta sezione ha ritenuto di concludere per l'imprescindibilità di un controllo giurisdizionale da svolgere nel nostro ordinamento in merito all'utilizzabilità dei dati probatori raccolti all'estero,

[13] V. MANZINI, *Diritto penale italiano*, VIII, Torino, 1947, p. 780.

[14] A questo riguardo, si è osservato come non possa ravvisarsi una differenza ontologica tra il contenuto di una conversazione o di una comunicazione e il documento che rivela i dati estrinseci di queste, quale il tabulato telefonico: documento che – come già rilevato in precedenza ad altro fine (sentenza n. 188 del 2010) – può aprire squarci di conoscenza sui rapporti di un parlamentare, specialmente istituzionali, «di ampiezza ben maggiore rispetto alle esigenze di una specifica indagine e riguardanti altri soggetti (in specie, altri parlamentari) per i quali opera e deve operare la medesima tutela dell'indipendenza e della libertà della funzione» (sentenza n. 38 del 2019).

aprendo solo all'alternativa tra carattere preventivo o successivo dello stesso. In particolare le questioni rimesse sono state così formulate: «1) Se l'acquisizione, mediante ordine europeo di indagine, dei **risultati di intercettazioni** disposte dall'Autorità giudiziaria estera su una piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.; 2) Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'Autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul "*server*" di una piattaforma criptata sia soggetta nell'ordinamento interno ad un **controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità** dei dati raccolti».

2. Il funzionamento dei sistemi SkyEcc e Encrochat e le indagini "a monte" delle autorità straniere.

La prima questione – di ordine metodologico - da risolvere è se sia possibile rispondere autenticamente a tali quesiti senza muovere dalla **conoscenza dell'esatto funzionamento dei sistemi SkyEcc o Encrochat e delle modalità con le quali l'AG straniera ha proceduto ad acquisire dette informazioni**[15]. Si anticipa che può apparire flebile e comunque non risolutiva la forza rassicurante che promana dal richiamo alla presunzione di conformità all'ordinamento dello Stato estero dell'esecuzione dell'attività acquisitiva, in nome del favore verso la cooperazione giudiziaria, così come non necessariamente autoevidente la capacità scientifica dell'algoritmo di decriptazione di produrre un solo risultato comprensibile, circostanza che dovrebbe costituire il segno dell'esattezza dell'estrazione del significato nascosto.

Ora, non sembra possibile conseguire risposte tranquillizzanti senza tener conto del **funzionamento dei sistemi cifrati di comunicazione** e dell'attività svolta dagli inquirenti esteri ancor prima di ricevere le richieste delle Procure italiane e di offrire loro risposta. **Conoscenze limitate** per profili essenziali e non agevolmente implementabili su profili anche decisivi, in presenza di operatività ormai interrotte e di fonti conoscitive affidate all'esperienza degli stessi "intrusori" avvalsisi del segreto per i maggiori dettagli.

Pur muovendo da tali problematiche premesse e volendo schiarire in breve l'operatività dei cd. "**criptofonini anti-intercettazione**" va considerato, anzitutto, quello considerato dalle varie pronunce della Cassazione per risolvere le questioni giuridiche sinora giunte al suo vaglio. Come ricorda da ultimo Cass., Sez. III, 47798/2023 tali apparati «sono da intendersi quali dispositivi smartphone che usano metodi di crittografia capace di proteggere i sistemi di comunicazione, solitamente basati, [..], sullo stesso hardware dei telefonini normali ma con l'aggiunta di sistemi di cifratura superiori ai normali dispositivi Android o Apple. I criptofonini utilizzano un ***hardware* standard**, in genere Android, Black Berry o IPhone, ma rispetto ai normali telefonini ospitano un ***software* capace di contenere un sistema operativo dedicato**, avente particolari requisiti di sicurezza, in quanto **disabilita servizi di localizzazione** (GPS, Bluetooth, fotocamera, scheda SD e porta USB). **Le chiamate rimangono attive ma solo in modalità Voice over IP** (VoiP)[16], **non**

[15] Siano esse poi state incorporate in documenti, di sostanza informatica, o in evidenze informatiche rappresentative di flussi di comunicazioni legalmente intercettati all'estero mentre i flussi erano in essere o in dati informatici costituenti corrispondenza o comunicazione che conservava per le parti direttamente coinvolte attuale interesse alla inviolabilità della libertà e segretezza, salvo motivato e legalmente emesso provvedimento da parte dell'A.G.

[16] Come ricorda M. RAMPIONI, *I limiti, cit.,* 4, nell'evoluzione dei sistemi di telecomunicazione uno sviluppo importante è stato rappresentato dalla possibilità di effettuare chiamate ed inviare messaggi sfruttando semplicemente la rete internet ed i suoi protocolli di trasmissione (VoIP), la cui tecnologia ha originato la diffusione di numerosissime applicazioni quali Skype, WhatsApp, Signal, WikrMe, Zfone, PrivateWave, utilizzabili sia mediante personal computer che tramite smartphone, per la realizzazione di comunicazioni in fonia, video-conference, senza limitazioni geografiche e senza costi. Tutte queste applicazioni si basano sull'utilizzo del protocollo TCP-IP che consente l'invio e la ricezione dei dati (incapsulati in "pacchetti") tra due terminali, sfruttando un protocollo denominato HTTP (Hypertext Transfer Protocol). La trasmissione dei dati avviene in maniera non crittografata e, dunque, consente l'eventuale intercettazione dei pacchetti trasmessi e ricevuti.

appoggiandosi alla **rete GSM**[17] ed impiegano applicazioni **proprietarie e criptate** (Encrochat, SkyEcc, Anom, no1bc, etc.) che utilizzano reti diverse dalla normale rete telefonica, e che **sono crittografate ad una cifratura a più livelli**[18]. Vengono in rilievo in questo contesto ed in sintesi, per quanto qui di interesse, quali strumenti di comunicazione**, chat del tipo peer-to-peer che non sono salvate su un server pubblico**. **I backup delle comunicazioni** vengono invece salvati **sul dispositivo criptato e su di un server dedicato** messo a disposizione degli utenti dall'azienda che fornisce il servizio. Anche **la SIM utilizzata è particolare e dedicata, connettendosi esclusivamente alla rete di server predisposta dal fornitore del servizio**. In tal modo i criptofonini sarebbero al sicuro da intercettazioni».

Anche la dottrina ha osservato che **l'impermeabilità di tali criptofonini alle intercettazioni** attiene anche al **captatore informatico** «che qui trova sbarrate tutte le sue consuete via d'accesso: nei criptofonini risultano, infatti, disattivati i servizi Google, la videocamera, il microfono, il sistema Bluetooth, la porta USB, il sistema di geolocalizzazione. Inoltre, questi dispositivi non sono agganciati alla tradizionale rete telefonica o telematica in quanto, per comunicare, si servono di piattaforme informatiche crittografate il cui funzionamento dipende dall'impiego di server gestiti da privati, spesso allocati all'estero. Da qui, la necessità di disporre delle chiavi di cifratura in assenza delle quali, i flussi comunicativi scambiati tramite i criptofonini si presentano come mere stringhe informatiche redatte secondo il sistema binario: cioè, a dire, sequenze di numeri prive di qualsiasi significato intellegibile ai più»[19].

La ricostruzione dei giudici di legittimità è puntuale salvo per un particolare che resta un po' in ombra: l'ordinaria **temporaneità della conservazione dei messaggi criptati sul *server* del fornitore del servizio**. Riepilogando, infatti, i telefoni forniti da SkyEcc, oltre ad avere fotocamere, microfoni e GPS disabilitati, tra le funzionalità note consentivano la trasmissione di messaggi crittografati che poi, **dopo trenta secondi, venivano automaticamente eliminati dal *server* dedicato dal fornitore del servizio**; se un telefono non fosse stato raggiungibile dalla rete, peraltro, il messaggio sarebbe stato conservato fino a 48 ore e poi cancellato; infine, l'utente poteva immettere una *password* "antipanico" e il dispositivo ne cancellava il contenuto. La funzionalità di **cancellazione periodica dal *server* dedicato**, dopo un brevissimo tempo di conservazione, induce a

---

[17] Nel 1995 in Italia è divenuta operativa la prima rete di comunicazioni radiomobili in tecnologia *GSM* (cd. tecnologia di generazione 2G) che ha apportato numerose innovazioni, tra le quali: la completa cifratura delle trasmissioni che impedisce intercettazioni illegali; una miglior efficienza spettrale che consente di usufruire di "servizi dati" come l'invio e la ricezione di messaggi di testo (Sms). La rete *GSM* è stata successivamente implementata dalle tecnologie *GPRS* ed *EDGE* (di generazione *2.5G*) grazie alle quali gli utenti possono usufruire, nell'ambito dei sistemi di messaggistica testuale di funzionalità per l'invio e la ricezione di file multimediali (video e messaggi vocali). Con l'ulteriore sviluppo delle reti radiomobili (tecnologia *UMTS, cd. 3G*) si può iniziare ad usufruire anche della videochiamata, della videoconferenza e della connessione alla rete internet che consente la navigazione sul Web. Le successive tecnologie standard LTE e 5G hanno ampliato ulteriormente le capacità comunicative in termini di velocità di trasmissione e ricezione dati. In tema cfr. M. RAMPIONI, *I limiti, cit.,* p. 4.

[18] Va ricordato che la Netscape Communication Corporation ha progettato a ed integrato il protocollo HTTPS che fornisce una cifratura bidirezionale delle comunicazioni, garantendo così che i contenuti delle comunicazioni non possano essere intercettati o alterati da terzi. L'unico modo per captare i messaggi e le comunicazioni "coperte" da cifratura è l'installazione di un *malware* sul telefono oggetto di interesse. In questo modo «l'agente intrusore» riesce ad operare in modalità "*fully- aquiring*", superando i sistemi di garanzia e consentendo di leggere direttamente quanto appare sul *display* prima che i dati vengano criptati. Proprio per contrastare questa eventualità, alcune aziende specializzate del settore hanno sviluppato soluzioni *stand-alone (Encrochat, Kline Plus*) implementando un'applicazione di messaggistica istantanea e/o di funzioni di chiamate su smartphone appositamente modificati nell'*hardware* e nel *software* per ostacolare l'inoculazione del captatore informatico. Gli smartphone modificati vengono venduti con applicazioni preinstallate, tra cui una di messaggistica basata su *OTR* (off-the-record, protocollo che fornisce la crittografia per le conversazioni di messaggistica istantanea), ed un servizio di chiamata vocale basato su *ZRTP* (Z-Real-Time-Transport- Protocol, protocollo che consente di effettuare chiamate criptate su rete internet). Proprio questa la tecnologia è usata dal sistema *SkyEcc.*

[19] L. LUDOVICI, I *criptofonini: sistemi informatici criptati e server occulti*, in Penale Diritto e Procedura, 2/2023, pp. 417-424.

ritenere probabile (o comunque maggiormente credibile) che gli accessi realizzati da parte delle autorità straniere a quest'ultimo – naturalmente ove l'acquisizione sia stata realizzata con intrusione presso quest'ultimo – siano avvenuti, secondo meccanismo funzionalmente omogeneo all'intercettazione rispetto di conversazioni/comunicazioni in atto[20].

Il sistema offerto da **EncroChat** era simile a quello proposto da SkyEcc. I *crypto-phone* venivano presentati ai clienti come una garanzia di assoluto anonimato e di completa discrezione tanto dell'interfaccia crittografata che del dispositivo in sé[21]. In primo luogo, non veniva eseguita alcuna associazione tra dispositivi o SIM e il conto del cliente. In aggiunta, i dispositivi presentavano un doppio sistema operativo, in modo che il sistema crittografato non fosse rilevabile. Infine, erano disabilitati il GPS, la fotocamera, il microfono e la porta USB. Anche le funzioni del sistema di messaggistica erano organizzate per aumentare la possibilità di occultare le comunicazioni: cancellazione automatica dei messaggi sui dispositivi destinatari, codice PIN specifico per eseguire la cancellazione di tutti i dati sul dispositivo, cancellazione di tutti i dati in caso di inserimento consecutivo di una *password* sbagliata. Inoltre, era possibile per gli utenti far cancellare i dati da remoto tramite l'assistenza del rivenditore.

Nonostante il carattere sofisticato di tali sistemi di protezione delle comunicazioni, tra il 2020 e il 2021, grazie all'impiego di squadre investigative di indagine costituite dalle autorità francese, olandese e belga, si è giunti alla **decriptazione** e allo **smantellamento** di due delle principali piattaforme criptate fino a quel momento conosciute, ossia proprio Encrochat e SkyEcc[22], con grande

[20] Ancora più in dettaglio, ricostruisce M.RAMPIONI, *op. cit.*, pp. 5 e ss.: «L'applicativo garantisce la sicurezza delle informazioni in questo modo: alla prima attivazione del dispositivo si generano le chiavi private (la *master key*) per la cifratura end-to-end; una volta inserita la password di sblocco il dispositivo verifica la sicurezza della connessione al Server (se vengono riscontrati problemi di sicurezza non è possibile utilizzare il sistema di messaggistica *SkyEcc*); all'esito positivo della verifica della sicurezza della connessione avviene lo scambio di chiavi e la successiva procedura di autenticazione al server; terminate queste fasi l'utente può iniziare a scambiare i messaggi di testo e a condividere i propri file multimediali. Rispetto ai primi apparecchi criptati, la piattaforma *SkyEcc* prevede, inoltre, ulteriori forme di «protezione»: quella della cancellazione automatica dei messaggi dopo trenta secondi; quella della conservazione del messaggio non recapitato per un massimo di quarantotto ore nel server (i cd. messaggi «autodistruttivi»); il cd. «*kill switch*» mediante cui si inserisce una password di panico che cancella l'intero contenuto del telefono; le SIM utilizzate sui propri dispositivi sono registrate e di sua proprietà, non consentendo così di risalire all'utente; nessun messaggio sarà mai, ed in ogni caso, conservato sul server per più di quarantotto ore».

[21] I *crypto-phone* venivano venduti intorno ai 1.000 euro ciascuno, con abbonamenti semestrali da 1.500 euro con supporto 24/7.

[22] Già nel 2017 la Gendarmeria e le autorità giudiziarie francesi avevano iniziato a indagare su questi telefoni dopo averne più volte riscontrato l'impiego da parte di gruppi della criminalità organizzata. Nel dicembre 2018 e nell'ottobre 2019, un giudice francese ha consentito alle autorità di **copiare i dati collegati al dominio EncroChat da un *server*** situato nella città francese di Roubaix. Una decrittazione parziale ha dimostrato che erano dati "al di là di ogni dubbio, legati ad attività illegali, in particolare al traffico di droga». Il 30 gennaio 2020 (e ancora il 12 febbraio) un giudice ha autorizzato l'installazione remota di uno **strumento di intercettazione** sui dispositivi degli utenti finali collegato al *server*. L'accusa ha affermato che ciò era necessario per identificare e arrestare gli utenti implicati attività illegali. Dopo aver ottenuto diverse altre autorizzazioni, le autorità hanno installato lo **strumento necessario per l'intercettazione, classificato segreto** per la difesa nazionale dal 1° aprile 2020. Dunque, **basandosi su un'estrazione del *server* di EncroChat** gli investigatori avevano sviluppato un **virus trojan che è stato inoculato all'interno del *server* stesso e poi all'interno dei dispositivi degli utenti sotto forma di un falso aggiornamento di sistema**. Su 64.134 utenti registrati ne sono stati intercettati 32.477 provenienti da 122 Paesi, di cui 380 in Francia e ben 4.600 in Germania. Pertanto, **tra aprile e giugno del 2020 le autorità francesi hanno potuto ottenere gli IMEI dei dispositivi, gli indirizzi e-mail degli utenti, la data e l'ora della comunicazione, l'ubicazione delle antenne attraverso le quali è stato effettuato l'accesso, nonché i testi e le immagini trasmessi nelle chat in corso**. Inoltre, è stata **letta la memoria completa dei dispositivi intercettati, accedendo anche alle chat dei periodi precedenti all'indagine e che non erano ancora state cancellate.** Solo in Francia, la Gendarmerie ha impiegato una *task force* di 60 uomini per monitorare le comunicazioni di migliaia di persone, avviando un elevato numero di procedimenti penali. Nei Paesi Bassi, al contempo, l'attività di centinaia di investigatori ha beneficiato delle informazioni estratte dalle chat ed è riuscita ad ottenere l'arresto di oltre 100 indagati, a smantellare 19 laboratori di droghe sintetiche, a sequestrare tonnellate di cocaina e *crystal meth*, nonché armi, veicoli e milioni di euro in contanti. L'**attività di intercettazione si è infine interrotta il 13 giugno del 2020**, quando EncroChat si è accorta della violazione dei sistemi da parte delle autorità e ha subito inviato un messaggio di allarme a tutti gli utenti.

impatto sui procedimenti di criminalità organizzata pendenti in Italia. Infatti, le Procure italiane hanno emesso numerosi OIE volti all'acquisizione, per il tramite dell'autorità giudiziaria francese, dei dati comunicativi ritenuti di interesse per l'accertamento dei reati perseguiti nei singoli procedimenti[23].

Va in proposito considerato, come già anticipato, che la **piattaforma SkyEcc** offriva in dotazione agli utenti, come ulteriore forma di «protezione», sim-card di sua proprietà che non consentivano di risalire (non immediatamente almeno) ai proprietari degli apparecchi mobili. L'anonimato garantito dalle schede telefoniche non precludeva, tuttavia, all'organo inquirente di venire a conoscenza del **luogo di utilizzo** (e dunque, **verosimilmente, anche degli utilizzatori**) dei sistemi crittografici; tale tecnologia, infatti, **sfruttava la convenzionale rete telefonica per inviare i messaggi, coinvolgendo**, come ogni altro sistema di comunicazioni, **le celle nazionali**; agganciando una data cella, le sim-card inserite nei diversi dispositivi «rilasciano» una serie di dati (i cd. dati esteriori di comunicazioni), tra cui il **codice IMSI** (International Mobile Subscriber Identity)**[24]** ed **IMEI** (International Mobile Equipment Identity) che, nelle diverse operazioni investigative, sono stati acquisiti dai diversi organi inquirenti nazionali per fini di polizia. I codici IMEI o IMSI, ad esempio, possono essere acquisiti dall'apprensione fisica del device (come avviene a seguito di sequestro), con dispositivi quali l'IMSI-catcher[25] o all'esito di analisi di celle o dati acquisiti previa autorizzazione giudiziale. I dati telefonici raccolti dagli investigatori italiani (i codici IMSI ed IMEI che contraddisti apparati nei quali riscontrata la predisposizione all'utilizzo di messaggistica criptata)[26], **incrociati con la massa delle risultanze probatorie fornite dall'A.G. francese** (i PIN associati agli IMEI e i messaggi già decodificati), hanno permesso di individuare i numerosi utilizzatori e possessori degli apparecchi telefonici criptati e comunicazioni con contenuti di rilievo penale. Da tali approfondimenti sono scaturiti, dunque, numerosi provvedimenti cautelari e indi molteplici pronunce della Cassazione.

Venendo al secondo ordine di questioni, un **primo orientamento** di legittimità assume **irrilevante approfondire le modalità dell'intrusione realizzata "a monte"**. Limitandosi a rimarcare che i criptofonini necessitano di una infrastruttura di *server* messi a disposizione dalla

[23] La Francia ha condiviso per la prima volta i dati con i Paesi Bassi, Eurojust ha facilitato la creazione di una squadra investigativa comune tra i due paesi con la partecipazione di Europol. Un esempio di buona pratica che ha fornito informazioni chiave per l'identificazione, le indagini e il procedimento giudiziario delle reti criminali. Nel rapporto preliminare di settembre 2021 si annota che sarebbero scaturiti 6.700 arresti e 3.800 procedimenti giudiziari; numero suscettibile di essere incrementato alla luce di numerose operazioni segnalate in Germania e Regno Unito, ma anche in Spagna, Italia, Paesi Bassi, Svezia e Belgio.

[24] L'IMSI è numero univoco associato a ogni utente di un dispositivo mobile, come uno smartphone o un tablet, che utilizza una rete cellulare. Esso è memorizzato nella scheda SIM (Subscriber Identity Module) del dispositivo e permette alle reti cellulari di identificare e autenticare gli utenti al fine di fornire loro i servizi. L'IMSI è composto da tre parti principali: MCC (Mobile Country Code): un codice di 3 cifre che identifica il paese in cui il dispositivo è registrato. MNC (Mobile Network Code): un codice di 2 o 3 cifre che identifica l'operatore di rete mobile a cui è abbonato l'utente. MSIN (Mobile Subscription Identification Number): un numero univoco assegnato dall'operatore di rete mobile che identifica l'utente all'interno della rete. La combinazione di MCC, MNC e MSIN forma un codice univoco che consente alle reti cellulari di identificare ogni singolo utente e gestire le loro comunicazioni e servizi. L'IMSI è dunque un'informazione sensibile, poiché può essere utilizzato per rintracciare e monitorare gli utenti. Le informazioni IMSI si trovano all'interno della scheda SIM (Subscriber Identity Module) del dispositivo mobile. La scheda SIM è una piccola scheda di plastica con un circuito integrato che contiene le informazioni dell'utente e viene inserita nel dispositivo mobile per permettere l'accesso alla rete cellulare. Le informazioni IMSI memorizzate nella SIM vengono utilizzate dagli operatori di rete mobile per identificare e autenticare gli utenti quando si connettono alla rete.

[25] È un dispositivo che si finge una cella di una rete mobile. In altri termini, quando un telefono cellulare cerca una rete nelle vicinanze, l'IMSI-catcher si presenta come la cella più attraente per il dispositivo, che si connetterà automaticamente a essa. Una volta stabilita la connessione, l'IMSI-catcher è in grado di intercettare le comunicazioni tra il dispositivo e la rete, incluse chiamate vocali, messaggi di testo e dati internet. L'IMSI-catcher non solo intercetta i dati, ma può anche localizzare la posizione del dispositivo, interrompere il servizio e in alcuni casi, iniettare malware o falsi messaggi nel dispositivo. Questo lo rende uno strumento molto potente per la sorveglianza e il monitoraggio delle comunicazioni.

[26] L'IMEI è legato esclusivamente al dispositivo in uso e non ha alcuna relazione di tipo permanente o semi-permanente con l'utente. L'identificazione di quest'ultimo all'interno della rete cellulare, invece, è affidata al codice IMSI contenuto nella scheda SIM.

compagnia che li produce, con relativo abbonamento. Ad esempio, la S.C. nella prima ordinanza di rimessione alle Sezioni Unite, ha ricordato: «Quanto alla piattaforma Sky-ECC, lo sforzo congiunto della polizia francese, belga ed olandese, coordinati da EUROPOL, ha permesso a quegli organismi di introdursi nella rete criptata Sky-ECC avendo accesso alle comunicazioni di soggetti dediti ad attività illecite. In particolare, il 9 marzo 2021 la polizia belga dava esecuzione ad una maxi operazione su base internazionale, così rendendo pubblica l'avvenuta violazione del sistema criptato Sky-ECC. Di fatto, l'operazione ha permesso di decrittare i contenuti delle chat scambiate dai criminali, avendo accesso ai flussi di informazioni di oltre 70.000 utenti, che la Cooperazione internazionale guidata da EUROPOL ha permesso». La S.C. è esplicita nel ritenere che "**non assume rilevanza**, ai fini del vaglio di legittimità del tipo di acquisizione in esame, **la questione se i dati stessi siano stati acquisiti dalla magistratura straniera *ex post* o in tempo reale** (quindi come "dati freddi" o come "flussi di comunicazioni"). Osservandosi, in sostanza, che **ciò che rileva è che i flussi di comunicazione non fossero più in corso al momento in cui sono stati chiesti i dati e** (a maggior ragione) **quando quei dati furono trasmessi dalla Autorità che li aveva acquisiti**. Per cui, in tal caso, la situazione non sarebbe dissimile da quella che si verifica quando viene acquisito *ex post* un flusso di comunicazioni, scritte o per immagini, memorizzato sulla memoria di un apparecchio telefonico[27].

Diverse sentenze di legittimità invece mostrano un **interesse per quanto avvenuto all'estero per iniziative delle autorità straniere** anche se poi muovono da una **presunzione di legittimità** di tale attività[28] - sostanzialmente - invincibile. Così viene chiarito che a monte l'Autorità giudiziaria francese ha proceduto ad una complessa e ramificata attività di intercettazione, eseguita attraverso un doppio passaggio e consistita, dapprima, nell'intercettare le comunicazioni intercorse sulla piattaforma SkyEcc, quindi nell'acquisire (tramite l'inoculazione nei *server* di appositi *trojan*) le chiavi di cifratura (due delle quali presenti nel *server* e due nel singolo cellulare dell'utilizzatore) idonee a consentire la decrittazione di tutte le conversazioni intercettate (necessarie per trasformare la comunicazione criptata in espressioni comprensibili). Tale attività di indagine, effettuata con riferimento ad ipotesi di reato relative, oltre che alla fattispecie di associazione finalizzata al traffico di stupefacenti, alla violazione della legge sui mezzi di crittografia, è stata autorizzata dalla competente Autorità giudiziaria francese (Giudice istruttore). Ciò è ritenuto sufficiente per rilevare come la procedura francese appaia, nell'ambito di tale ordinamento, legittimamente eseguita, «considerato, da un lato, il principio di diritto, già affermato in tema di rogatorie, secondo il quale gli atti probatori trasmessi dall'Autorità giudiziaria straniera si presumono (*iuris tantum*) legittimi, riservando al giudice straniero la verifica della correttezza della procedura e la risoluzione delle relative questioni (da ultimo, Sez. 3, n. 1396 del 12/10/2021 - dep. 2022, Torzi, Rv. 282886 - 01); dall'altro lato, il fatto che le procedure di indagine compiute in Francia sono state riconosciute legittime dai supremi organi giurisdizionali di quel Paese (Cour de Cassation, sentenza del 2 aprile 2022; Conseil Costitutionel, decisione n. 2022-987 QPC dell'8 aprile 2022)». Tale conclusione è stata affermata anche da una recente sentenza della Corte (Sez. 6, n. 48838 del 11/10/2023, dep. 07/12/2023, Brunello, n.m.) che ha rilevato che «nel sistema delineato dalla direttiva 2014/41/UE, l'autorità di emissione dell'ordine europeo di esecuzione non può sindacare la legittimità delle misure mediante le quali lo Stato di esecuzione ha raccolto le prove, in quanto spetta ai giudici dello Stato di esecuzione conoscere dei ricorsi giurisdizionali avverso tali atti e che all'autorità giudiziaria italiana spetta, dunque, solo verificare se l'ordine europeo di indagine sia stato legittimamente emesso secondo le previsioni della direttiva 2014/41/UE e della disciplina interna di recepimento, il d.lgs. 21 giugno 2017, n.108, e se le prove acquisite mediante la cooperazione internazionale siano utilizzabili nel procedimento penale interno» (nello stesso senso, in merito alla legittimità del procedimento svolto in Francia, v. Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, n.m. che ha evidenziato come la Corte costituzionale di quel Paese ha statuito che le norme processuali interne applicate nel caso in

[27] Cass., Sez. IV del 16/05/2023 n. 38002/23 n.m. cit.
[28] Cass., Sez. VI, n. 2329/2024.

esame sono «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»).

Non mancano **sentenze di legittimità più "curiose" rispetto a quanto avvenuto Oltralpe**. A tale ordine di pronunce vanno annoverate, ad esempio, quelle che ritengono importante **chiarire se l'A.G. francese abbia avviato le indagini nel proprio Paese autonomamente**, sulla base di preesistenti *notitiae criminis,* oppure se le investigazioni siano state attivate (anche) sulla base delle **sollecitazioni istruttorie contenute negli OEI del pubblico ministero italiano**[29]. Così è stato richiesto di precisare, in sede di rinvio, se, rispetto al momento della emissione e della trasmissione di tali ordini, le indagini compiute dall'A.G. francese fossero state tutte definitivamente concluse, oppure se fossero proseguite anche sulla base delle richieste formulate dall'A.G. italiana. Non potrebbe parlarsi di acquisizione di "dati freddi" (elementi relativi a comunicazioni già avvenute e memorizzati nei "*server*" della società "SKY-ECC" presenti in Francia) quella avvenuta in presenza del compimento di un'ulteriore attività investigativa disposta dall'A.G. Nei diversi casi giudiziari, la difesa aveva segnalato intercettazioni di comunicazioni in corso, con impiego di captatori informatici (c.d. "*trojan*" o "*malware'*') utilizzate per l'acquisizione di dati di comunicazione telematica archiviati nel "*server*" di quella società e per consentire l'apprensione delle "chiavi di decifrazione" presenti negli apparecchi utilizzati dai fruitori della piattaforma di messagistica cifrata in questione; nonché attività di sequestro (pur non comprendendosi se di interi sistemi informatici ovvero solo dei relativi dati, "riversati" su altri supporti di materiale a disposizione della suddetta società). E ciò valeva ai fini della verifica della utilizzabilità processuale di elementi di prova acquisiti all'estero con uno o più OEI, in ragione del "**principio di equivalenza**" previsto dall'art. 6, par. l, lett. b), della Direttiva 2014/41/UE, 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».

La rilevanza delle modalità di acquisizione viene sostenuta anche secondo diverso percorso argomentativo, riflesso delle più recenti indicazioni della **Corte di Giustizia europea** in materia di **dati esteriori delle comunicazioni,** convergenti verso l'applicabilità ad essi delle garanzie previste dall'art. 15 Cost. in materia di intangibilità della riservatezza delle comunicazioni. Sono «dati esteriori di comunicazioni» una serie di informazioni di varia natura, suscettibili di acquisizione e di utilizzazione processuale, che attengono non solo ai dati relativi alle telefonate su apparecchi fissi o mobili, ma anche ad ogni altro tipo di comunicazione elettronica. Dati personali qualificati perché forniscono retrospettive di rilievo (il tempo, la durata, la frequenza delle chiamate, le utenze contattate, i codici IMEI, gli intestatari delle SIM e l'ubicazione dell'utenza mediante la geolocalizzazione storica delle celle di aggancio) consentendo di creare una mappatura incisiva di una parte rilevante dei comportamenti privati di una persona. In ragione della loro capacità intrusiva la Corte costituzionale, sin dalla sentenza n. 81 del 1993, ha riconosciuto, in forza dell'art. 15 Cost., il diritto di mantenere segreti sia i dati suscettibili di condurre all'identificazione dei soggetti della conversazione, sia quelli relativi al tempo e al luogo della comunicazione[30]; nondimeno, ritenendo che l'acquisizione dei dati esteriori comprimesse in maniera minore il diritto di cui all'art. 15 Cost. rispetto alla captazione delle conversazioni, il giudice delle leggi ha ritenuto sufficiente che all'acquisizione del dato procedesse il pubblico ministero con decreto motivato, in linea con la disciplina del sequestro di corrispondenza. In materia di intangibilità della riservatezza delle comunicazioni passi più decisi vengono compiuti dalla Corte di Giustizia, in linea con le pronunce della Corte Europea dei diritti dell'Uomo[31], delineando limiti per l'acquisizione dei dati in questione.

[29] Cass., Sez. IV, n. 44154/2023.

[30] C. cost., sentenza 11 marzo 1993, n. 83, in www.cortecostituzionale.it, massima n. 19298; in linea cfr. C. cost., sentenza 28 maggio n. 2010, n. 188, in *www.cortecostituzionale.it*; C. cost., 6 marzo 2019, n. 38, in *www.cortecostituzionale.it*, massima n. 42192.

[31] C. edu, Copland c. Regno Unito, 3 aprile 2007, par. 44, in *www.europeanrights.com*; C. edu, Barbulescu c. Romania, 5 settembre 2017, par. 74, in *www.europeanrights.com*.

Approfondendo i principi già affermati in materia di *data retention*[32], la **Grande Sezione della Corte di Giustizia, con la sentenza del 2 marzo 2021, H.K. c. Prokuratuur**[33] ha fissato i criteri ai quali gli Stati membri devono soggiacere per consentire l'accesso da parte dell'autorità pubblica ai dati conservati dai fornitori, per bilanciare esigenze di prevenzione, accertamento e repressione dei reati con la tutela del diritto alla riservatezza dei cittadini. Per tale sentenza la direttiva 2009/136/CE, letta alla luce degli artt. 7, 8 e 11 nonché dell'art 52, par. 1, della Carta dei diritti fondamentali dell'Unione Europea, osta: *i*) ad una normativa nazionale che consenta alle autorità pubbliche l'accesso a dati relativi al traffico o a dati relativi all'ubicazione per finalità di prevenzione, ricerca, accertamento e perseguimento dei reati senza che tale accesso sia circoscritto a procedimenti aventi per scopo la lotta contro forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza; *ii*) a una normativa nazionale che investa il pubblico ministero della competenza ad autorizzare l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione al fine di condurre un'istruttoria penale. Per tali ragioni, per evitare che pratiche illegittime di acquisizione di dati, o la loro conservazione generalizzata ed indifferenziata, possano arrecare pregiudizio a una o più persone che, in quel dato momento storico, ben potrebbero non essere sospettate (neppure indiziate) di aver commesso reati[34] nonché per escludere informazioni ottenute in violazione delle prescrizioni del diritto dell'Unione funzionali a garantire il rispetto del principio del contraddittorio e, dunque, del diritto ad un equo processo, è necessario un **controllo preventivo rimesso a un giudice o a un'autorità amministrativa indipendente e terza rispetto alle parti pubbliche e private**. Ad avviso della CGUE il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica, come rilevato in sostanza dall'Avvocato generale al paragrafo 126 delle sue conclusioni, che l'autorità incaricata di tale controllo preventivo, da un lato, **non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale.**: " Ciò **non si verifica nel caso di un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale**. Infatti, il pubblico ministero non ha il compito di dirimere in piena indipendenza una controversia, bensì quello di sottoporla, se del caso, al giudice competente, in quanto parte nel processo che esercita l'azione penale. La circostanza che il pubblico ministero sia tenuto, conformemente alle norme che disciplinano le sue competenze e il suo *status*, a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento non può essere sufficiente per conferirgli l*o status* di terzo rispetto agli interessi in gioco nel senso descritto al punto 52 della presente sentenza. L'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso **osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale[35].** Ne consegue che il pubblico ministero non è in grado di **effettuare il**

[32] Corte di Giustizia, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C- 698/15, *Tele2 Sverige AB*; Corte Giustizia, Grande Sezione 8 aprile 2014, cause riunite C-293/12 e C-594/12 *Digital Right Ireland*.

[33] Pronunciandosi sul rinvio pregiudiziale formulato dalla Corte Suprema estone in ordine all'interpretazione dell'art. 15, par. 1, dir. 2002/58/CE – relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche – come modificata dalla direttiva 2009/136/CE del Parlamento Europeo e del Consiglio, del 25 novembre 2009.

[34] F.R. DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in Proc. pen. e giust., 2022, vol. 2, p. 314.

[35] Dalla decisione della Corte di Giustizia del 2 marzo 2021 è scaturito un vivace dibattito giurisprudenziale. La Corte di Cassazione, con due arresti della seconda sezione penale (Cassazione Penale, Sez. II, 15 Aprile 2021, n.28523, e Sez. II, 2 luglio 2021, n. 33116), ha **escluso l'applicazione diretta della sentenza della CGUE GS** atteso il generico riferimento

controllo preventivo di cui al punto 51 della presente sentenza[36]. Sulla scorta dei principi enunciati dalla Corte di Giustizia il legislatore italiano ha adotta in via di urgenza il D.L. 30 settembre 2021, n. 132[37].

Ai fini della presente trattazione da tale ricostruzione scaturirebbe una "nuova" **forma di inutilizzabilità di «derivazione comunitaria"** affiancata a quelle scaturenti dalla **violazione dei principi costituzionali**»[38] che imporrebbe ai giudici nazionali di escludere dal compendio probatorio informazioni ed elementi di prova ottenuti illegittimamente (o conservati in maniera generalizzata e indifferenziata). Tale impostazione può confliggere con quella che giustifica la legittimità delle

---

ai casi nei quali i tabulati di traffico telematico e telefonico possono essere acquisiti con conseguenti profili di incertezza interpretativa. I giudici di legittimità, pur non dubitando della possibile diretta applicabilità nell'ordinamento nazionale dei principi espressi nella sentenza del 2 marzo 2021, H.K., C-746/18, in considerazione del valore fondante del diritto comunitario con efficacia erga omnes nell'ambito della Comunità da attribuirsi agli stessi (cfr. Cass., Sez. Lav., n. 13425 del 2019; Cass. Civ, n. 22577 del 2012), hanno ritenuto tuttavia che l'attività interpretativa del significato e dei limiti di applicazione delle norme comunitarie, operata nelle sentenze CGUE, può avere efficacia immediata e diretta nel nostro ordinamento limitatamente alle ipotesi in cui non residuino, negli istituti giuridici regolati, concreti problemi applicativi e correlati profili di discrezionalità che richiedano l'intervento del legislatore nazionale, tanto più laddove si tratti di interpretazioni di norme contenute nelle direttive (cfr., Sez. 2, n. 28523 del 15/04/2021, Lordi, non mass.). L'indeterminatezza delle espressioni utilizzate dalla CGUE, al fine di legittimare l'ingerenza dell'autorità pubblica nella vita privata dei cittadini ("lotta contro le forme gravi di criminalità" o "prevenzione di gravi minacce alla sicurezza pubblica"), implicava necessariamente, secondo la Corte di cassazione, un intervento legislativo volto ad individuare, sulla base di «criteri oggettivi», così come richiesto dalla stessa pronuncia della Corte europea, le categorie di reati per i quali possa ritenersi legittima l'acquisizione dei dati di traffico telefonico o telematico. L'orientamento della Corte di Cassazione non appariva in contrasto con la sentenza della Corte di Giustizia che ai §§ 48-50 riconosce che spetta al diritto nazionale stabilire le condizioni dell'accesso ai dati prevedendo regole "chiare e precise", idonee a soddisfare il requisito di proporzionalità, che disciplinino 3 la portata e l'applicazione della misura in questione e fissino requisiti minimi, non potendosi "limitare a esigere che l'accesso ai dati risponda alla finalità perseguita, ma dovendo prevedere le condizioni sostanziali e procedurali che disciplinano tale utilizzo".

[36] Dalla sentenza della CGUE in commento: «§ 50: "Pertanto, e poiché un accesso generale a tutti i dati conservati, indipendentemente da un qualche collegamento, almeno indiretto, con la finalità perseguita, non può considerarsi limitato allo **stretto necessario**, la normativa nazionale in questione deve fondarsi su 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. A questo proposito, un accesso siffatto può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per 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. Tuttavia, in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone potrebbe essere parimenti concesso qualora sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo (v., in tal senso, sentenze del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 119, nonché del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 188). § 51. Al fine di garantire, in pratica, il pieno rispetto di tali condizioni, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate. In caso di urgenza debitamente giustificata, il controllo deve intervenire entro termini brevi (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 189 e la giurisprudenza ivi citata)».

[37] Il legislatore, intervenuto in via d'urgenza con il d.l. nr. 132/2021, ha modificato l'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, sottoponendo al controllo del giudice la procedura di acquisizione dei dati, relativi al traffico telefonico e telematico per fini di indagine penale, e la selezione dell'ambito oggettivo di applicazione della procedura stessa, esperibile solo in relazione ai procedimenti per reati puniti con l'ergastolo o con pena edittale massima non inferiore a tre anni, e per i reati di minaccia, molestie e disturbo a mezzo telefono, quando la minaccia, la molestia e il disturbo sono gravi, sempre che ricorra la rilevanza investigativa del dato da acquisire. La novella si attesta sule coordinate essenziali con la disciplina sulle intercettazioni (artt. 266 e ss. c.p.p.) richiedendo tuttavia, in ragione della più contenuta invasività del mezzo, la sufficienza e non la gravità indiziaria, in relazione ai delitti per i quali si ammettono le operazioni, la rilevanza anziché l'assoluta indispensabilità investigativa dei dati stessi ed ampliando i termini per la convalida del giudice nei casi d'urgenza da 48 a 72 ore.

[38] F. R. DINACCI, *L'acquisizione*, cit., p. 314; S. MARCOLINI, *Le indagini atipiche nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 775.

procedure poste in essere per l'acquisizione dei dati sottoforma di documentazione informatica; se infatti, è indubbio che a monte esistevano i **provvedimenti autorizzativi di giudici di francesi** (di Lille e di Parigi) **per le intercettazioni telefoniche[39] gli stessi non riguarderebbero affatto l'intera massa delle captazioni** (quali quelle per cui oggi si procede in Italia), bensì solo una serie di comunicazioni afferenti reati di criminalità organizzata e terrorismo compiuti in Francia nell'anno 2021. Gran parte della **messaggistica sarebbe stata acquisita con la tecnica investigativa della "pesca a strascico"** (in contrasto con **l'art. 270 c.p.p.)**[40] **in assenza di una notizia di reato, in mancanza dei relativi – specifici e collegabili - provvedimenti autorizzativi**[41] **e conservata su appositi *server* in maniera generalizzata ed indifferenziata**. A fronte del dovere delle autorità straniere di assicurare, immediatamente e compatibilmente con le indicazioni unionali, la cancellazione dal *server* di convoglio di tutte le chat per cui non c'era autorizzazione alle intercettazioni[42], secondo alcune ricostruzioni i giudici nazionali dovrebbero comunque dichiarare l'inutilizzabilità della messaggistica SkyEcc, riconoscendo l'incompatibilità delle procedure acquisitive poste in essere dall'autorità giudiziaria transalpina con le norme inderogabili dell'ordinamento interno e per la violazione dei principi sanciti dalla Corte di Giustizia in materia di intangibilità delle comunicazioni.

Come si vedrà nelle pagine successive, la consapevolezza della gravità delle conseguenze ha persuaso la giurisprudenza italiana a preferire soluzioni che offrono soddisfazioni parziale a talune delle esigenze di conoscenza e di approfondimento, tenuto altresì conto che in sede di legittimità lo spazio di considerazione di esse presuppone chiaramente tratteggiati i contenuti delle doglianze e un interesse concreto a conseguirne il vaglio giudiziale.

Occorre dire che, entro certi limiti, resta oscuro **cosa sia avvenuto all'estero per iniziativa delle autorità inquirenti straniere e**, in particolare, **con quali esatte modalità esse si siano procurati i dati poi trasferiti alle autorità italiane**. In particolare, non conoscendo lo strumento tecnologico della captazione non è dato sapere esattamente in che modo si sia giunti all'acquisizione dei messaggi criptati, ossia se, attraverso la captazione di flussi in fase dinamica ovvero mediante l'acquisizione di dati telematici "freddi", cioè già archiviati nella memoria del *server* (ipotesi che invero per quanto detto appare meno plausibile). A questo proposito, secondo alcune indicazioni giurisprudenziali i messaggi sarebbero stati decrittati perché la società che ne era proprietaria avrebbe messo a disposizione degli investigatori gli algoritmi e le chiavi di cifratura. La spiegazione è ritenuta implausibile in punto di fatto: «non si deve, infatti, dimenticare che i criptofonini attenzionati usavano il sistema di **crittografia *end to end*** che, a differenza di quello denominato *pin to pin*, si serve di chiavi di cifratura depositate non all'interno del *server* ma direttamente nei dispositivi: ciò significa

[39] Trib. di Reggio Calabria, Sez. per il Riesame delle misure cautelari personali, Ord. 19 novembre 2022, n. 868, p. 8.

[40] Proprio per evitare che le intercettazioni costituiscano uno strumento per sottoporre a monitoraggio la totale sfera personale del soggetto interessato e i soggetti che con quest'ultimo dovessero, anche casualmente, conversare viene esclusa un'utilizzazione completa del materiale acquisito. Non potendo operare a monte, essendo impossibile limitare la sfera tecnologica del mezzo intercettizio attivato, il legislatore è intervenuto a valle stabilendo una griglia per l'utilizzabilità del materiale acquisito. Tale opzione di intervento si è svolta attraverso una lettura restrittiva dell'utilizzazione del materiale acquisito a mezzo delle intercettazioni limitando l'agibilità processuale dello stesso a quanto oggetto di specifica autorizzazione (e valutazione motivata) dell'autorità giudiziaria. Precipitato concreto e stringente di tale presupposto è che vi è un divieto di utilizzazione delle risultanze intercettizie in procedimenti diversi da quelli nei quali le stesse sono state disposte. Assume, pertanto, un rilievo fondamentale l'esatta declinazione della definizione "procedimento diverso".

[41] Base giuridica di questo vincolo si trarrebbe proprio dall'art. 270 c.p.p. che nella vigente formulazione statuisce: «I risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza».

[42] Nella disciplina francese in materia di intercettazioni, analogamente a quella italiana, l'autorizzazione emessa dal Giudice istruttore deve indicare tassativamente: *i*) gli elementi necessari ad identificare le comunicazioni passibili di captazione; *ii*) il reato in relazione al quale è disposta l'attività di ricerca della prova; *iii*) la relativa durata dell'attività di captazione. Ciò indipendentemente se si procede nelle forme previste dall'art. 100 c.p.p. francese o 706-102-1 c.p.p. francese, nella sua formulazione risultante dalla legge 23 marzo 2019.

che non è tecnicamente possibile che la società proprietaria del *server* abbia potuto fornire agli investigatori l'algoritmo per decriptare le stringhe informatiche, trattandosi di un dato ad appannaggio esclusivo degli utenti del servizio cioè i proprietari dei *devices*. Per questo motivo sembra da condividere la tesi – avanzata in dottrina – secondo la quale la captazione dei flussi comunicativi in questione sarebbe avvenuta in questo modo: attraverso l'inoculazione di un malware all'interno del server per il successivo invio di una notifica *push* – che cioè perviene al destinatario senza bisogno di download – verso i criptofonini che, quindi, dialogando con il server di gestione, avrebbero automaticamente trasmesso le chiavi di cifratura agli investigatori»[43]. Così non pochi commentatori (e in parte alcune prime ricostruzioni giurisprudenziali) ritengono indubbio che se per acquisire dati esterni di comunicazioni (dati relativi al traffico e all'ubicazione ai fini di un'istruttoria penale) vi è necessità dell'autorizzazione di un giudice indipendente (dal pubblico ministero che, per usare le parole della CGUE, dirige il procedimento istruttorio penale ed esercita, eventualmente, l'azione penale in un successivo procedimento**)** non facilmente potrebbe escludersi ragioni di assimilazione con dati pertinenziali e strettamente funzionali (come le **chiavi di cifratura**) alla volontà di nascondere il contenuto di comunicazioni. E poco differenzierebbe la situazione il fatto che i dati trasmessi con l'OEI sarebbero già messaggi decriptati, ossia i risultati di un'operazione (decrittaggio) che presuppone l'applicazione dell'algoritmo di decifratura alle chiavi crittografiche pertinenziali.

3. I temi in campo: lo strumento processuale "interno" per importare le "chat" decrittate oggetto dell'OEI, la competenza ad autorizzare l'attività di indagine e ad avanzare la richiesta di cooperazione sino all'ambito del controllo giurisdizionale interno.

3.1. Il protocollo dell'art. 234-*bis* c.p.p. ed i corollari.

Nella quasi totalità dei casi i messaggi sono stati richiesti all'A.G. francese con OEI emessi dalle Procure italiane, con decriptazione realizzata attraverso l'individuazione dell'algoritmo utilizzato dalla società proprietaria del sistema di cifratura Sky-Ecc. Molte sentenze della Cassazione hanno condiviso la legittimità di tale schema acquisitivo respingendo le doglianze difensive volte a rimarcare la violazione degli artt. 266 c.p.p. per assenza di autorizzazione del Gip all'effettuazione di intercettazioni, sottolineando, piuttosto, la **natura documentale** (non captativa) delle chat fornite dal Tribunale di Parigi. In particolare, l'attività è stata qualificata nei termini di acquisizione di **dati "freddi"** ovvero estranei, nella loro acquisizione, ad un flusso di comunicazioni in corso.

In particolare molte pronunce del giudice di legittimità hanno stabilito che l'acquisizione, mediante OEI, di messaggi su chat di gruppo presso A.G. straniera che ne abbia già eseguito la decrittazione ad oggetto "**documenti e di dati informatici**" ai sensi dell'art. 234-*bis* c.p.p.[44]. In particolare, la tesi muove dalla **distinzione**, di rilievo per le comunicazioni criptate, tra **intercettazioni**, da una parte, e **acquisizione e decifrazione di dati comunicativi**, dall'altra. In proposito, le **operazioni di captazione e di registrazione** del messaggio cifrato (nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario) vanno distinte dalle **operazioni di acquisizione del contenuto del messaggio** già inoltrato oltre che di **decriptazione** dello stesso, necessarie per trasformare mere stringhe informatiche in dati comunicativi intellegibili. Solo alla prima tipologia fa riferimento l'art. 266-*bis* c.p.p., che estende l'applicabilità delle norme del codice di rito relative alle "normali" intercettazioni di conversazioni o comunicazioni tra soggetti a distanza, alle intercettazioni di **flussi** di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici (flussi, cioè, che non avvengono in via diretta tra apparecchi informatici, ma che sfruttano la trasmissione dei dati in via telematica, dunque via cavo o ponti radio, ovvero per mezzo

[43] L. LUDOVICI, I *criptofonini,* cit. 419.

[44] Tra le tante, Cass., sez. IV, n. 37503 del 30/05/2023 n.m.; Id., sez. IV del 16/05/2023 n. 38002/23 n.m; Id., sez. IV, n. 16345 del 05/04/2023, Liguori ed altri, non mass.; Id. Sez. IV, n. 16347 del 05/04/2023 Rv. 284563- 01; Id., Sez. l, n. 6364 del 13/10/2022 (dep. 15/02/2023) Rv. 283998- 01.

di altra analoga strumentazione tecnica)[45]. Laddove, invece, il **messaggio telematico sia acquisito allorquando non sia più all'interno di un flusso in corso di comunicazioni** e sia stato criptato va esclusa la disciplina delle intercettazioni, destinata ad operare solo per i flussi di comunicazioni in atto[46] e gli inquirenti ne possono valorizzare il contenuto a fini dimostrativi, disponendo dell'algoritmo che consente di decriptarne il tenore ovvero acquisendo tale "chiave" dalla società che ne è proprietaria.

Del resto, gli assimilabili **messaggi "whatsapp"** e **sms conservati nella memoria di un telefono cellulare** integrano **mera documentazione di detti flussi**[47] costituendo rappresentazioni comunicative incorporate in una base materiale con un metodo digitale, ovvero dati informatici che consentono la intelligibilità del contenuto di stringhe redatte secondo il sistema binario[48]. Attività non rientrante tra le operazioni di intercettazioni, perché non riguardante la captazione e la registrazione di dati comunicativi *in itinere* dal mittente al destinatario.

In questa prospettiva, **non assume rilevanza**, ai fini del vaglio di **legittimità del tipo di acquisizione in esame, la questione se i dati stessi siano stati acquisiti dalla magistratura straniera *ex post* o in tempo reale** (quindi come "dati freddi" o come "flussi di comunicazioni"). Ciò che **rileva è che i flussi di comunicazione non fossero più in corso al momento in cui chiesti i dati** e (a maggior ragione) **quando quei dati furono trasmessi dalla Autorità che li aveva acquisiti.** Situazione non dissimile da quella che si verifica quando viene acquisito *ex post* un flusso di comunicazioni, scritte o per immagini, memorizzato sulla memoria di un apparecchio telefonico[49].

Dalla natura delle chat quali dati o documenti informatici di tipo comunicativo conseguirebbero **rassicuranti premesse** circa la legittimità dell'acquisizione delle medesime tenuto conto del principio di equivalenza, ove già ottenute e conservate da A.G. estera, **mediante OEI attivato dal Pubblico ministero.** L'**art. 234-*bis* c.p.p.**, in particolare, costituirebbe la norma interna di riferimento, alla stregua della quale verificare l'esistenza del potere di procedere con l'OEI, che può avere ad oggetto solo atti d'indagine richiesti che "avrebbero potuto essere emessi in un caso interno analogo", secondo la direttiva 2014/41/UE cit. Tale norma troverebbe applicazione in quanto viene in rilievo l'acquisizione non di un documento cartaceo o analogico, bensì di un documento inteso come «rappresentazione comunicativa incorporata in una base materiale con un metodo digitale»[50].

Rispetto alla questione se l'acquisizione in esame, ai fini della utilizzabilità dei dati in tal modo versati in atti, presupponga una preventiva o comporti una successiva **verifica giurisdizionale** della sua legittimità **da parte del giudice nazionale**, dall'illustrata impostazione conseguirebbe la piena legittimità dell'ottenimento dei documenti informatici in parola, attraverso un atto, l'OEI, attivato dal Pubblico ministero, **senza necessità** di **ulteriori verifiche giurisdizionali interne**, anteriori e tantomeno posteriori, rispetto alla citata acquisizione[51].

Come annota in argomento, in termini più ampi, la Cassazione nella prima ordinanza di rimessione alle Sezioni Unite (sent. n. 47798/2023), «si deve premettere che l'Ordine europeo d'indagine è disciplinato dal d.lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva

---

[45] Cfr. in motivazione, Cass. Sez. VI, n. 18907 del 20/04/2021 Rv. 281819 - 01; nel medesimo senso quanto all'acquisizione dei contenuti di messaggistica in atto, effettuata con sistema Blackberry, cfr. Cass. Sez. IV, n. 49896 del 15/10/2019, Rv. 277949-01; Sez. III, n. 47557 del 26/09/2019, Rv. 277990-01, 02; Sez. III, n. 50452 del 10/11/2015, Rv. 265615-01.

[46] Cfr. Cass., Sez. IV, n. 16347 del 05/04/2023 Rv. 284563 - 01.; Id., Sez. I, n. 34059 del 01/07/2022, non mass.; Sez. VI n. 18907 del 20/04/2021, Rv. 281819 - 01 cit.; Id., n. 22417 del 16/3/2022, Rv. 283319; Id., n. 28269 del 28/05/2019 Rv. 276227 - 01; Id., Sez. III, n. 29426 del 16/4/2019, Rv. 276358; Id., Sez. V, n. 1822/2019, Rv. 272319.

[47] In tale ultimo senso, tra le altre, cfr. Cass., Sez. VI n. 1822/2020, Rv. 278124 - 01; Id., Sez. V, n. 1822/2018 Rv. 272319.

[48] Cass. Sez. VI, n. 18907/2021, Rv. 281819, cit., in motivazione; Sez. I, n. 6364/2023, Rv. 283998, in motivazione.

[49] Cass. Sez. IV del 16/05/2023 n. 38002/23 n.m. cit.

[50] Fra le altre, in particolare, Cass. Sez. I - n. 6364/2023 Rv. 283998 — 01 cit.

[51] Cfr. per tutte, sul tema, Cass. Sez. I, n. 6364/2023, Rv. 283998 — 01.

2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014. L'Ordine europeo d'indagine, per quanto qui di interesse, "può anche essere emesso per ottenere **prove già in possesso delle autorità competenti dello Stato di esecuzione**" (art. 1, punto 1 della direttiva suindicata). Inoltre, secondo gli artt. 6 e 9 della direttiva citata, l'OEI può avere ad oggetto, come sopra già riportato, solo atti d'indagine richiesti che "avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo" e l'autorità di esecuzione riconosce l'O.E.I., "senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione, a meno che non decida di addurre uno dei motivi di non riconoscimento o di non esecuzione ovvero uno dei motivi di rinvio previsti dalla presente direttiva". Consegue, alla luce di tali principi, la ricostruzione giurisprudenziale per cui, da una parte, nel caso in esame si tratta non di una richiesta di procedere ad intercettazioni, ma di una **richiesta di acquisizione degli esiti documentali di attività d'indagine precedentemente svolta**, rispetto alla quale l'ordinamento interno rinviene la **piena ed esclusiva competenza del P.M**.; **organo peraltro competente** nella fase di indagine, salve specifiche eccezioni, quali la richiesta di effettuazione di intercettazioni all'estero (art. 43 del d.lgs. n. 108 del 2017), all'emissione dello stesso OEI. Per cui la competenza esclusiva del P.M. nell'effettuare, nell'ordinamento interno, l'acquisizione in parola, trova riflesso anche nella analoga richiesta rivolta all'estero mediante OEI».

Prosegue ancora Cass. 47798/2023, cit.: «Inoltre, l'utilizzazione degli atti trasmessi a seguito di attività di cooperazione internazionale **non è condizionata da un accertamento ad opera del giudice italiano della regolarità delle modalità di acquisizione esperite dall'Autorità straniera**, in quanto vige la **presunzione di legittimità dell'attività svolta** 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[52]. In altri termini, l'OEI, oltre a dover avere ad oggetto una prova acquisibile nello Stato di emissione, deve eseguirsi in conformità a quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria, e si deve presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario[53]. Il **giudice italiano**, quindi, **non può e non deve conoscere della regolarità degli atti di esecuzione di attività di indagine compiuta dall'autorità giudiziaria straniera** (nel caso di specie quella francese), **giacché detta l'attività investigativa è eseguita secondo la legislazione dello Stato estero**; e, **a maggior ragione,** ciò vale 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»**. Secondo la tesi in esame, dunque, si tratta di una **richiesta di acquisizione degli esiti documentali di attività d'indagine che l'Autorità straniera ha già svolto, nella sua piena autonomia, nel rispetto della sua legislazione in relazione ad altri reati**; pertanto, **la tutela giurisdizionale relativa a tali atti trova spazio solo in tale diverso ordinamento**.

In ogni caso, andrebbe riconosciuto che in materia di OEI vige il principio di diritto, già espresso in tema di rogatoria internazionale, secondo cui trovano applicazione, da un lato il principio "*locus regit actum*" e; dall'altro, in conformità ai canoni di diritto internazionale, quello della prevalenza della "*lex loci*" sulla "*lex fori*". Ciò si porrebbe in linea con la più recente evoluzione normativa internazionale e sovranazionale, volta a rendere più snella ed efficace la mutua assistenza giudiziaria e funzionale e diretta a superare quest'ultimo concetto con quello di "cooperazione" per una più efficace lotta contro il crimine transnazionale. Ciò sul presupposto della sostanziale conformità degli ordinamenti degli Stati europei agli stessi principi di tutela dei diritti fondamentali della personae e sulla base della mutua fiducia nella capacità degli Stati stessi di garantire un equo processo, come avvalorato dal fatto che in materia di cooperazione giudiziaria in ambito dell'Unione

[52] In tal senso, Cass. Sez. V, n. 1405/2017, Rv. 269015; Sez. II, n. 24776/2010, Rv. 247750 - 01; Sez. I, n. 21673/2009, Rv. 243796 – 01.
[53] Tra le altre, Cass. Sez. VI, n. 48330 del 25/10/2022, Rv. 284027, in motivazione.

Europea vige il principio del mutuo riconoscimento[54] che implica una presunzione di conformità (al sistema europeo) delle diverse legislazioni nazionali.

Né viene considerato di pregio l'argomento inerente all'**asserita incompatibilità delle chat così acquisite rispetto al diritto interno**, nella misura in cui si faccia riferimento alla necessità di verificare che all'attività investigativa di cui si tratta nello Stato estero abbia provveduto un giudice e non un pubblico ministero, 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 l. 23 novembre 2021, n. 178. Ciò in ragione (e ancor prima della eventuale verifica dell'intervento, in ogni caso, all'estero, dell'A.G. ai fini della acquisizione dei dati in parola), del rilievo per cui ciò che viene acquisito, nel quadro in esame, sono **documenti informatici** e **non "dati esteriori"**[55]. È su queste basi, così sintetizzate, che si esclude dunque, secondo un diffuso orientamento di legittimità, che **l'acquisizione in esame debba essere oggetto, ai fini della utilizzabilità dei dati versati in atti, di preventiva o successiva verifica della sua legittimità da parte del giudice nazionale**.

Corollari della suesposta tesi della acquisibilità, nel quadro dell'art. 234-*bis* c.p.p. di messaggi su chat di gruppo presso l'A.G. straniera che ne abbia eseguito la decrittazione sono inoltre, in sintesi, anche i seguenti principi, variamente rinvenibili nelle decisioni di legittimità. Si tratta: *i*) della legittimità del ricorso, per chiedere la trasmissione di documentazione già acquisita dall'A.G. estera ad un OEI **emesso dal PM nazionale**; *ii*) della rinvenibilità del **consenso** all'acquisizione dei dati, da parte del "**legittimo titolare**" di quei documenti conservati all'estero, come previsto dall'art. 234-*bis* c.p.p., nell'assenso che proviene dal soggetto che di quei documenti o di quei dati poteva disporre: da intendersi come persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del Paese estero, identificabile non soltanto nella **persona fisica e/o giuridica** che procede alla trasmissione e alla conservazione dei dati, ma anche nella **polizia giudiziaria**, **nell'autorità giudiziaria**[56], nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*internet service provider*[57]; *iii*) dell'**esclusione,** salvo allegazione di specifici e concreti elementi di segno contrario, della ricorrenza **di alterazioni o manipolazioni dei testi captati anche in assenza della fornitura dell'algoritmo necessario**, in quanto secondo la **scienza informatica**, risulterebbe impossibile, ove la chiave di decrittazione non fosse corretta, ottenere un testo avente un significato intellegibile sebbene difforme da quello reale, potendosi, al più, imbattersi in una sequenza alfanumerica o simbolica (detta "stringa") priva di senso alcuno[58]; *iv*) dell'affidamento della **garanzia del rispetto dei diritti fondamentali**, nell'ambito del procedimento di cui all'O.E.I., **in primo luogo allo Stato membro di emissione**, che si deve **presumere rispetti il diritto dell'Unione**.

3.2. Le critiche al protocollo dell'art. 234-*bis* c.p.p. e il favore per l'inquadramento nell'art. 254-*bis* c.p.p., con le conseguenze.

---

[54] Per una panoramica cfr. la bibliografia citata da M. RAMPIONI, cit., p.10 Tra gli altri, sul tema, S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo*, in T. RAFARACI (a cura di), *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia, Atti del convegno, Catania, 9-11 luglio 2005*, Milano, 2007, p. 691; L. MARIN, *Il principio del mutuo riconoscimento nello spazio penale europeo,* Napoli, 2006, p. 78.

[55] Il riferimento è ai tabulati, dei quali le Sezioni Unite n. 21 del 13/07/1998, Gallieri, Rv. 211196 - 01, hanno offerto una utile definizione, precisando che "essi costituiscono la documentazione in forma intellegibile del flusso informatico relativo ai dati esterni al contenuto delle conversazioni". Cfr. Cass., Sez. I, n. 6364/2023, Rv. 283998 - 01 cit.

[56] Tribunale di Reggio Calabria, Sezione per il Riesame delle misure cautelari personali, Ord. 5 novembre 2022, n. 801

[57] In motivazione Cass. Sez. I, n. 6364 del 13/10/2022 Rv. 283998 - 01 cit.

[58] In motivazione Cass., Sez. IV, n. 30395 del 21/04/2022 Rv. 283454 - 01; sullo stesso tema e sul diritto di difesa in tema di decrittazione di dati informatici anche Cass., sez. VI, n. 14395 del 27/11/2018 (dep. 02/04/2019) Rv. 275534 – 01.

In termini critici è stato osservato che l'art. 234-*bis* c.p.p. prevede due tipologie di acquisizione dati: *i*) la libera acquisizione di dati informatici disponibili e fruibili attraverso la semplice navigazione in rete, per scelta consapevole o meno dell'interessato, condivisi da un numero indeterminato di soggetti[59]; *ii*) l'acquisizione di dati conservati all'estero e non liberamente fruibili, ossia quei dati informatici che il titolare non ha voluto diffondere sulla rete e che ha inteso mantenere riservati su apposite piattaforme, alle quali è possibile accedere solamente con l'utilizzo di *password* o di cifrature, dato che in sede processuale sono utilizzabili unicamente se acquisiti con il "consenso del legittimo titolare". L'estensione di quest'ultimo concetto all'ampia categoria dei soggetti che esercitano sui dati informatici diritti soggettivi è da più parti della riflessione dottrinale avversata in favore di una sua limitazione all'usuario del dispositivo che ha stipulato il contratto con la società di riferimento (SkyEcc) o al gestore del servizio (la società Sky Global) che ha contratto apposite intese contrattuali con l'utente ed ha disponibilità dei dati informatici e delle chiavi di decriptazione; impostazione già sostenuta dalla Cassazione con riferimento ad altra tipologia di strumentazione criptata (basta aper vero su diverse basi tecnologiche) dei cd. dispositivi Blackberry[60]. Per contro le Autorità francesi non sono considerate in alcun modo titolari dei dati informatici in questione, ma al più "detentrici" a seguiti di acquisizione (mediante installazione di un *malware* nei *server* di riferimento) coattiva da uno dei legittimi titolari (l'azienda SkyEcc) nell'ambito di una specifica attività d'indagine. Per tale ragione nell'acquisizione dei messaggi decriptati sembrerebbe difettare il requisito del consenso del legittimo titolare richiesto dall'art. 234-*bis* c.p.p.

Altre sentenze della Sesta Sezione della Corte di Cassazione hanno aperto a orientamenti dissenzienti rispetto alle suesposte soluzioni in ordine alle due questioni sottoposte all'esame delle Sezioni Unite. Con la sentenza n. 44154/2023, Rv. 285284, in presenza di caso peculiare (nel provvedimento gravato non era stato chiarito se rispetto al momento della emissione e della trasmissione degli O.E.I., le investigazioni compiute dall'A.G. francese fossero state tutte definitivamente concluse, oppure se fossero proseguite anche sulla base delle richieste formulate dall'A.G. italiana, in presenza di documentazione di attività di indagine dell'autorità straniera) la S.C. ha ritenuto che l'art. 234-*bis* c.p.p. sarebbe inapplicabile in presenza dei risultati di un'attività acquisitiva che, anche in attuazione della richiesta di assistenza formulata dall'A.G. italiana, si sia concretizzata nell'**apprensione occulta del contenuto archiviato in un *server* ovvero nel sequestro di relativi dati ivi memorizzati o presenti in altri supporti informatici**, nella disponibilità della società che gestiva quella piattaforma di messaggistica. Attività acquisitiva, piuttosto, inquadrabile nelle disposizioni in materia di **perquisizione e sequestri**, in specie nell'art. **254-*bis* c.p.p.**, riguardante le ipotesi di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

La premessa nitida su questa ricostruzione è che l'operatività dell'art. 234-*bis* c.p.p. «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». La delimitazione della predetta fattispecie *ex* art. 234-*bis* c.p.p. alla sola acquisizione di dati informatici in ogni caso estranei, nella loro formazione, a qualsivoglia coinvolgimento di autorità investigative, contraddice il diffuso e diverso indirizzo sopra esposto, secondo cui ciò che invece importa, per la rilevanza della norma citata, è che i flussi di comunicazione non fossero più in

[59] S. ATERNO, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nelle privacy*, in *Archivio Penale*, 1/2016, p. 165 «rientrano in questa categoria, ad esempio, i dati relativi ai profili pubblici sui social network, il contenuto di un sito web o di un blog, le fotografie pubblicate su piattaforme di condivisione a livello mondiale, i messaggi lasciati on line nei gruppi di discussione pubblici e altri dati simili. La caratteristica che hanno tutte queste informazioni è che per scelta consapevole (a volte inconsapevole) dell'interessato o dl proprietario del dato stesso, essi sono condivisi con una sfera indeterminata di soggetti».

[60] Cass., Sez. IV, 26 ottobre 2022, n. 49411, in *www.dejure.it*.

corso al momento in cui sono stati chiesti i dati e (a maggior ragione) quando quei dati furono trasmessi.

Non mancando però pronunce relative all'acquisizione dalla Francia delle "chat" transitate sulla piattaforma SkyEcc nelle quali la Cassazione ha già escluso che possa ritenersi applicabile l'art. 234-*bis* c.p.p. Così Cass., Sez. VI, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363 - 03, assume che «in tema di prove informatiche, l'art. 234-*bis* cod. proc. pen. - che, a fini di contrasto al terrorismo, ha trasposto la regola di cui all'art. 32 della Convenzione sul "*cybercrime*", ratificata con legge 18 marzo 2008, n. 48 - non è applicabile nel caso di prove documentali acquisite mediante ordine europeo di indagine - nella specie, messaggistica tratta dalla piattaforma criptata "Sky Ecc" - in quanto tale norma consente di acquisire documentazione digitale reperibile in rete da fonti aperte, salva la necessità di consenso del titolare del documento in caso di accesso protetto, senza il ricorso a procedure di collaborazione con lo Stato ove i documenti geograficamente si trovano». Da Cass., Sez. VI, n. 48838/2023, Brunello, cit., si è evidenziato come la sentenza della Corte costituzionale n. 170 del 2023 ha statuito che le chat costituiscono forme di corrispondenza e non già meramente «documenti di dati informatici»[61].

A tali considerazioni è stato aggiunto (Cass., Sez. VI, n. 2329/2024) che l'art. 27, par. l, della citata Convenzione di Budapest, concernente le procedure relative alle richieste di mutua assistenza giudiziaria in assenza di accordi internazionali applicabili, esclude la possibilità di applicare, tra la Parte richiedente e quella richiesta, le norme pattizie (ivi comprese quelle dettate dall'art. 34 della Convenzione, relativo alle intercettazioni di dati relativi al contenuto delle comunicazioni),"qualora vi sia un trattato, un accordo o legislazione in vigore" (nel caso in esame, evidentemente, la *lex specialis* sarebbe rinvenibile nella direttiva 2014/41/UE e nelle correlate norme di recepimento in Italia e in Francia), a meno che le Parti interessate siano d'accordo nell'applicare al loro posto, in tutto o in parte, le norme convenzionali previste dalla suddetta disposizione.

Secondo detto orientamento giurisprudenziale, anche da ultimo ribadito (Cass., Sez. VI, n. 48838/2023, cit.), **nel caso di specie non potrebbe farsi riferimento alla disciplina delle intercettazioni**, poiché la stessa presuppone l'esistenza di flussi di comunicazioni in atto (in senso conforme, Cass., Sez. VI, n. 46482 del 27/09/2023, Bruzzaniti, cit., che ha precisato "trattarsi di registrazioni di conversazioni già avvenute e, quindi, di dati "statici" assimilabili a corrispondenza, e non invece di intercettazioni). In effetti, tale ultima tipologia di atto di indagine - nell'ambito della procedura "attiva" - è contemplata espressamente nell'art. 43 d.lgs. cit., che ha dato attuazione all'art. 30 della citata Direttiva, ove si prevede al comma l che "Il pubblico ministero emette ordine di indagine, secondo il modello di cui all'allegato A, sezione H 7, del presente decreto, per la necessaria assistenza tecnica all'esecuzione delle operazioni di intercettazione delle conversazioni o comunicazioni o del flusso di comunicazioni relativo a sistemi informatici o telematici, quando nel territorio di altro Stato membro si trova il dispositivo o il sistema da controllare" (e, dunque, non potrebbe che riferirsi alle intercettazioni da effettuare e non all'acquisizione dei risultati di quelle precedentemente e autonomamente svolte dalla Autorità giudiziaria straniera). La fattispecie processuale potrebbe rientrare, dunque, nella **acquisizione di "corrispondenza informatica"** (le "chat", già disponibili, appunto, nello Stato di esecuzione attraverso il precedente ricorso a mezzi di intercettazione). D'altronde, si aggiunge, l'art. l, par. l, della direttiva 2014/41 UE consente il ricorso

[61] Cass. Sez. VI, n. 46833 del 26/10/2023, Bruzzaniti, n. m., nell'escludere la configurabilità dell'art. 234-*bis* c.p.p. ha affermato che tale articolo «introdotto nel 2015, invece, specifica ulteriormente l'art. 32 della Convenzione di Budapest sul cybercrime, già vigente nell'ordinamento in forza della legge di ratifica n. 48 del 2008 sopra menzionata, e consente in ogni caso 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. Tale disposizione, che mira a rendere agevole l'acquisizione della documentazione reperibile via internet, quindi, non è rilevante allorché le prove documentali digitali siano state formalmente consegnate dall'Autorità giudiziaria straniera, come nel caso in esame», concludendo per la sussistenza nella specie di una «acquisizione di documenti ai sensi dell'art. 234 cod. proc. pen.».

all'OEI anche per l'acquisizione di prove che già sono in possesso delle competenti Autorità dello Stato di esecuzione e il successivo art. 13 della direttiva disciplina il "**trasferimento delle prove**" (comprese quelle "**già in possesso dello Stato di esecuzione**"). Secondo questa tesi, si tratterebbe, dunque, di atti probatori già nella disponibilità dell'A.G. francese, che li ha acquisiti con procedura conforme al proprio ordinamento. In questa ottica, si è affermato che, a tal fine, «il **pubblico ministero può emettere l'ordine europeo di indagine** con cui si richiede il **trasferimento di dati documentali, in particolare di corrispondenza già acquisita in un procedimento penale nel paese membro di esecuzione**, per il cui **sequestro** è sufficiente, ai sensi dell'art. 15 Cost. e secondo le disposizioni interne, il **provvedimento motivato del pubblico ministero**, senza necessità di intervento del giudice per le indagini preliminari»[62]. Ove si ritenesse fondata tale opzione ermeneutica, la norma di riferimento dovrebbe essere individuata, dunque, nell'art. 254-*bis* c.p.p., che consente il sequestro di corrispondenza informatica.

Peraltro, anche in questo caso potrebbe porsi (sempre ai fini del rispetto del principio di "equivalenza") il problema di valutare la legittimità - secondo il nostro ordinamento - dell'attività di **sequestro "massivo" del contenuto dei "*server*" operato dalla Autorità giudiziaria francese, anche se si tratterebbe di controllo successivo**. Al riguardo, infatti, si è ritenuto (Cass., Sez. VI, n. 6623/2021, Pessotto, Rv. 280S38 - 01) che «È illegittimo, per violazione del **principio di proporzionalità ed adeguatezza**, il sequestro a fini probatori di un dispositivo elettronico che conduca, in difetto di specifiche ragioni, alla indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione degli eventuali criteri di selezione», essendosi peraltro precisato che «in tema di sequestro di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede[63]». Pertanto, ove dovesse ritenersi accoglibile tale ricostruzione normativa, si renderebbe comunque necessaria una **valutazione del Giudice cautelare in merito alla sussistenza**, nel caso concreto, dei requisiti di necessaria proporzionalità e adeguatezza nel nostro sistema processuale (profili, di contro, ritenuti chiaramente esistenti nell'ordinamento francese, attesa la natura illecita *in re ipsa* dell'attivazione e utilizzo della piattaforma Sky ECC).

A favore di questo diverso inquadramento sembra aver inciso l'**evoluzione registrata dalla normativa nazionale per l'acquisizione presso il *server* dei dati esterni alle telecomunicazioni**, dopo gli arresti della **Corte di giustizia dell'Unione europea**[64]; con l'adozione in via d'urgenza (d.l. n. 132 del 2021, convertito dalla l. n 178/2021) delle novelle disposizioni inserite nell'art. 132 Cod. privacy, è stata "**giurisdizionalizzata**" **la procedura** di acquisizione dei dati esterni di traffico telefonico e telematica (richiedendo un provvedimento autorizzatorio motivato del giudice). Così da concludere che l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione dovrebbe essere **sempre autorizzata da un giudice**: «sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematica 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». Conclusione assunta anche tenendo conto della posizione assunta dalla Corte costituzionale in ordine all'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**), considerata anche in collegamento con le posizioni assunte in materia dalla **Corte europea dei diritti dell'uomo** che ha ricondotto "sotto il

[62] Cass. Sez. VI, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363- 01.
[63] Cass., Sez. VI, n. 34265 del 22/9/2020, Aleotti, Rv. 279949; per riferimenti alle modalità operative si rinvia anche a Cass. Sez. VI, n. 13165 del 4/3/2020, Scagliarini, Rv. 279143.
[64] Corte di Giustizia, Grande Camera, del 2 marzo 2021 H.K., C-746/18.

cono di protezione dell'art. 8 CEDU", ove pure si fa riferimento alla "corrispondenza" *tout court*, i messaggi di posta elettronica[65] e la messaggistica istantanea inviata e ricevuta tramite internet[66].

Neppure gli effetti di questa diversa impostazione sono completamente condivisi presso il giudice di legittimità. Ad avviso della Sezione che ha per prima rimesso gli atti alle Sezioni Unite (Cass. sez. III 47798/2023) si tratta di affermazione, che al di là del riferimento ad una attività investigativa che pare diversa da quelle considerate dalla tesi in precedenza illustrata, sembra poter aprire la riflessione sul **necessario intervento, anteriore o postumo del giudice, per l'acquisizione all'estero dei dati comunicativi in parola**, richiedendo, la necessità, per il giudice del rinvio, di "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[67]. A giudizio della sentenza della Cassazione 2329/2024, cit., ove si utilizzi il paradigma dell'art. 254-*bis* c.p.p. (in alternativa a quello dell'art. 270 c.p.p.) sarebbe comunque legittima **l'adozione dell'OEI da parte del P.M**. Invero, l'acquisizione tanto della "corrispondenza informatica" quanto delle risultanze di intercettazioni disposte in altro procedimento deve ritenersi certamente consentita nel nostro ordinamento al P.M. Inoltre, appare condivisibile l'osservazione formulata nelle conclusioni rassegnate dall'Avvocato Generale presso la Corte di Giustizia il 26 ottobre 2023 nell'ambito del procedimento relativo al rinvio pregiudiziale disposto dal Tribunale di Berlino, secondo il quale ove lo **Stato di esecuzione ha disposto l'atto probatorio con provvedimento di un giudice**, **non è necessario che l'ordine di indagine europeo diretto al trasferimento di tali prove sia emesso da un giudice**, anche nel caso in cui, ai sensi del diritto dello Stato di emissione, la raccolta delle prove alla base dell'OEI avrebbe dovuto essere disposta da un giudice[68].

3.3. L'acquisizione come documenti *ex* art. 234 c.p.p.

Ulteriore indirizzo, nell'escludere l'applicabilità della disciplina sulle intercettazioni *ex* artt. 266 e ss. c.p.p., a fronte di O.E.I. avente ad oggetto la richiesta, all'A.G. straniera, di specifici «dati freddi», cioè documenti costituenti l'esito delle comunicazioni memorizzate su server, già acquisiti e decriptati dai giudici stranieri, in un loro procedimento autonomamente avviato e concluso (secondo una procedura peraltro garantita), ha elaborato una prospettazione ulteriore, rispetto a quelle sinora illustrate (Cass., sez.VI n. 46833/2023). Si è infatti sostenuto, pur considerando, alla luce della sentenza della C. cost. n. 170 del 2023, che anche la messaggistica informatica conservata dopo la ricezione costituisce e mantiene il carattere di corrispondenza[69], che anche quest'ultima, pure ove informatica, rientra nel fuoco dell'art. 234 c.p.p. Con esclusione, quindi, del riferimento all'art. 234-*bis* c.p.p., disposizione non conferente.

Infatti, mentre nella specie, si ha riguardo ai risultati di un'attività investigativa concretizzatasi nell'acquisizione di documenti di altro procedimento penale, svoltosi all'estero, attraverso una forma di collaborazione internazionale, l'art. 234-*bis* cit. è stato introdotto nel 2015 e specifica ulteriormente

---

[65] Corte EDU, sent. 5/09/2017, Barbulescu c. Romania, § 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, § 41; per gli SMS cfr. Corte EDU, sent. 17/12/2020, Saber c. Norvegia, § 48.

[66] Cfr. Corte EDU, sent. Barbulescu, cit., § 74.

[67] Quanto alla seconda sentenza della sesta sezione di questa Corte, n. 44155 del 26/10/2023 (dep. 02/11/2023) Rv. 285284 - 01, essa sembra ripercorrere l'impostazione della precedente, pur in assenza di espliciti riferimenti, anche solo di natura dubitativa, come avvenuto con la precedente decisione, al contenuto della ordinanza allora impugnata quanto alla concreta attività svoltasi all'estero a seguito di O.E.I. del Pubblico ministero italiano.

[68] Va ricordato che per Cass., Sez. VI, n. 2329/2024, cit., le prove richieste e trasferite nel nostro ordinamento sono state acquisite dallo Stato di esecuzione sulla base di una complessa e prolungata attività di intercettazione in precedenza svolta dalla Autorità francese e non a seguito di un sequestro di corrispondenza dalla stessa operata.

[69] Permanendo l'interesse alla riservatezza di tale messaggistica, "almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento storico".

l'art. 32 della Convenzione di Budapest sul *cybercrime*, già vigente nell'ordinamento in forza della l. di ratifica n. 48 del 2008, consentendo in ogni caso 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. In pratica, la Convenzione avrebbe introdotto la possibilità di acquisire la documentazione esistente in rete senza dover fare ricorso al sistema delle rogatorie internazionali o ad altri strumenti di cooperazione giudiziaria internazionale. Tale disposizione, che mira a rendere agevole l'acquisizione della documentazione reperibile via internet, non sarebbe rilevante, secondo la citata sentenza, allorquando le prove documentali digitali siano state formalmente consegnate dall'A.G. straniera, come nelle più parte dei casi in esame. Con l'ulteriore rilievo per cui, comunque, stabilire se l'acquisizione sia stata disposta ai sensi dell'una o dell'altra disposizione, riguarda profili meramente definitori, in concreto irrilevanti. Con altra sentenza (Cass., n. 46482 del 27.09.2023 dep. 17.11.2023) la Sesta Sezione della Cassazione ha condiviso il punto suesposto rilevando che, secondo quest'impostazione, l'art. 234-*bis* c.p.p. nulla aggiunge ai fini dell'accesso alla documentazione con i comuni mezzi (come il sequestro o la consegna diretta) e certamente il riferimento al "legittimo titolare" non significa che le legittime modalità di acquisizione delle prove siano condizionate dall'autorizzazione del "proprietario" del documento. Oltre a concludere nel senso per cui anche nella relazione tra Stati, cui si applica la disciplina O.E.I., quando la prova sia già stata acquisita con atto del giudice nel paese di esecuzione, il semplice trasferimento della prova preesistente nel procedimento in Italia, come da regole interne, può essere disposto sulla base della **sola richiesta del P.M.**

3.4. L'acquisizione quale attività di intercettazione.

Sulla scia delle indicazioni della sentenza n. 170/2023 della Corte costituzionale, una diversa opinione riconduce l'acquisizione delle chat alla **disciplina delle intercettazioni** (artt. 266 e 266-*bis* c.p.p.). Ciò in linea con un pregresso orientamento di legittimità, in tema di e-mail e di chat Blackberry, che riteneva attività di intercettazione l'acquisizione dei messaggi già spediti o ricevuti dall'indagato e conservati nelle rispettive caselle di entrata e uscita o nei *server* Blackberry situati in Canada. In particolare, il discrimine identificativo di un flusso informatico – rilevante per l'applicazione della disciplina delle intercettazioni – si identificava nell'avvenuto inoltro del messaggio da parte del mittente[70]. Dato atto della presenza di opinioni dissenzienti[71], aderendo a tale impostazione esegetica, inevitabili sarebbero le **ripercussioni** sul fronte dell'inutilizzabilità processuale dei dati Sky-Ecc acquisiti, ai sensi dell'art. 234-*bis* c.p.p., tramite OEI: *i*) violazione dell'art. 15 Cost. secondo cui la limitazione delle comunicazioni può avvenire solo nei casi e modi previsti dalla legge e per atto motivato dell'autorità giudiziaria, con conseguente e totale elusione delle norme previste in materia di intercettazioni; *ii*) **inutilizzabilità della prova estera**, secondo

[70] Era ritenuta legittima l'acquisizione di contenuti di attività messaggistica - nella specie, effettuata con sistema Blackberry - mediante intercettazione operata ai sensi degli artt. 266 ss. c.p.p., poiché le chat, anche se non contestuali, costituiscono un flusso di comunicazioni»; cfr, Cass. Sez. III, 10 novembre 2015, n. 50452, in C.E.D. Cass, n. 265615; Cass. Sez. IV, 28 giugno 2016, n. 40903, in C.E.D. Cass., n. 268228. Tale orientamento sembrerebbe trovare conferma in una risalente pronuncia delle Sezioni Unite, 13 luglio 1998, Gallieri, in C.E.D. Cass, n. 211197, con cui si invitava a valutare appieno la portata innovativa della l. 23 dicembre 1993, n. 547 sui *computer crimes*, con cui è stato introdotto l'art. 266-*bis* c.p.p. La sentenza Gallieri ha evidenziato che la telefonia, in specie mobile, consente il trasporto di segnali non solo relativi alle conversazioni, ma di qualunque tipo, sempre in forma numerica, cioè di dati diversi dal contenuto delle conversazioni telefoniche. E di tali dati deve attualmente ritenersi consentita l'intercettazione in virtù proprio dell'art. 266-*bis* c.p.p.

[71] Cfr. Cass., Sez. VI, 28 maggio 2019, n.28269, in www.dejure.it; Cass., Sez. VI, 6 febbraio, 2020, n.12975, in Cass. Pen., 2020, 12, p. 4664 «In tema di mezzi di prova, i messaggi di posta elettronica memorizzati nell'account o nel computer del mittente ovvero del destinatario hanno natura di documenti informatici, sicché la loro acquisizione processuale non soggiace alla disciplina delle intercettazioni di cui all'art. 266-*bis* c.p.p., che postula la captazione di un flusso di comunicazioni in atto, ma avviene ai sensi dell'art. 234 c.p.p.».

valutazione governata dalle regole dettate dall'ordinamento in cui la stessa è chiamata ad esprimere il suo contenuto conoscitivo[72], la cui applicazione imporrebbe al giudice italiano di vanificarne il risultato, riconoscendo la prova (acquisita dalla Francia) in contrasto con i principi dell'ordinamento nazionale[73].

3.5. L'acquisizione dei risultati delle intercettazioni eseguite da autorità straniera, la verifica del rispetto delle condizioni *ex* artt. 270 e 271 c.p.p. e i corollari.

Secondo un'ultima, alternativa, l'importazione delle chat decriptate costituirebbe "**acquisizione dei risultati di intercettazioni effettuate dall'A.G. francese**". L'art. 43, comma 3 e 4 d.lgs. n. 108/2017 espressamente contempla la possibilità che all'OEI possa darsi esecuzione, alternativamente, con la trasmissione immediata delle telecomunicazioni (ovvero con l'intercettazione, la registrazione e la successiva trasmissione dei risultati delle operazioni) o attraverso l'attività di trascrizione, decodificazione o decrittazione delle comunicazioni intercettate (evidentemente già in possesso dell'A.G. destinataria dell'ordine di indagine). Sebbene si tratti di disposizione dettata in riferimento alla procedura "attiva" dell'OEI, essa costituirebbe regola generale, valevole anche per l'OEI ricevuto in materia dall'A.G. italiana (artt. 23 e 24 d.lgs. cit.). Probabilmente la richiesta di trascrizione, decodificazione o decrittazione delle comunicazioni intercettate (art. 43, comma 4, cit.) dovrebbe essere più correttamente interpretata come formulazione di un'istanza collegata ed accessoria a quella, principale, contenuta nell'ordine di indagine richiesto ad altro Stato membro, al fine di intercettare una delle diverse forme di telecomunicazioni descritte nel primo comma dell'art. 43, come tali non già precedentemente acquisite nell'ordinamento richiesto, ma ancora da espletare e trasmettere, in via immediata (art. 43, comma 3, lett. a) o successiva (art. 43, comma 3, lett. b), in conseguenza della richiesta emessa in fase attiva dalle autorità italiane. Secondo la prospettiva in esame, gli **artt. l, par. l, 10, par. 2, lett. a), 13, par. l, della direttiva OEI**, e le correlate disposizioni attuative di cui agli **artt. 2, comma l, lett. a), 9, comma 5, lett. a), 10, comma l, 12, comma l, d.lgs. 108/2017**, fanno univocamente riferimento alla acquisizione di verbali di prove di altro procedimento e, dunque, anche di dati probatori già raccolti mediante la intercettazione di telecomunicazioni in altro Stato membro dell'UE, perché in precedenza autonomamente effettuate ed ivi già disponibili[74]. In questo caso, la norma di riferimento interna sarebbe l'**art. 270 c.p.p.**, che **regola la "importazione" dei risultati delle intercettazioni effettuate in diverso procedimento**. Anche se l'ordinamento processuale francese non contempla una

[72] Annota F.R. DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Milano, 2008, p. 144: «La prospettiva non si pone in contrasto con l'obbligo di osservanza della *lex loci* stabilito dall'art. 3, comma 1, della Convenzione europea di assistenza giudiziaria. Tale obbligo, infatti, non viene violato dal momento che l'assunzione della prova all'estero viene effettuata secondo le regole di quello Stato. Ma la situazione, risulta evidente, non preclude alla giurisdizione utilizzatrice delle prove estere un giudizio sulla legalità delle forme assuntive. Del resto, tale possibilità è ribadita dalla stessa rilevanza della legge del luogo, la quale non potrà che essere quella nell'ambito del quale il dato conoscitivo viene utilizzato».

[73] R. MARCHETTI, *L'assistenza giudiziaria internazionale*, Milano, 2005, p. 43, rimarca che la materia probatoria risulta intimamente connessa al profilo dei diritti e delle garanzie difensive, che non possono essere sacrificati per il solo fatto che l'assunzione probatoria abbia luogo in territorio straniero piuttosto che nello Stato in cui pende il procedimento.

[74] L'**art. 10, comma 2, lett. a), della Direttiva** consente «l'acquisizione di informazioni o prove che sono già in possesso dell'autorità di esecuzione quando, in base al diritto dello Stato di esecuzione, tali informazioni o prove avrebbero potuto essere acquisite nel quadro di un procedimento penale o ai fini dell''OEI» e il successivo **art. 13, comma 1**, stabilisce che «l'autorità di esecuzione trasferisce senza indebito ritardo allo Stato di emissione le prove acquisite o già in possesso delle autorità competenti dello Stato di esecuzione in esito all'esecuzione dell'OEI». L'**art. 9, comma 5, lett. a), d.lgs. 108/2017, cit**., a sua volta stabilisce che si provvede "in ogni caso" all'esecuzione dell'OEI avente ad oggetto "l'acquisizione di prove di altro procedimento", mentre l'**art. 12, comma l, d.lgs. cit.** prevede espressamente che "Il procuratore della Repubblica trasmette senza ritardo all'autorità di emissione i verbali degli atti compiuti, i documenti e le cose oggetto della richiesta, nonché i verbali di prove o gli atti acquisiti in altro procedimento". Tali ultime disposizioni appaiono espressione di principi che trovano fondamento nelle suindicate previsioni generali della Direttiva, sicché ben possono costituire, unitamente ad esse, canoni di orientamento alla cui stregua valutare la legittimità della predetta acquisizione, a mezzo OEI, degli esiti delle intercettazioni.

disposizione analoga al nostro art. 270 c.p.p., in "via pretoria" ha ammesso il trasferimento dei risultati dell'attività di intercettazione disposta in un diverso procedimento; profilo in ogni caso eccepibile dinanzi all'A.G. dello Stato di esecuzione. La legittimità della "trasposizione" dei risultati delle intercettazioni "aliene" andrebbe dunque valutata alla luce della **nostra disciplina processuale** (*ex* art. 270 c.p.p.) **sull'utilizzabilità delle relative comunicazioni**, considerando se le chat sono "rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza" (tra di essi rientrando i delitti di cui agli artt. 73 e 74 d.P.R. n. 309 del 1990) o, si ritiene, la ricorrenza di connessione sostanziale forte *ex* 12 c.p.p. (condizione che esclude che possa considerarsi "diverso" il procedimento ove emessa l'autorizzazione e quello relativo al reato accertato in forza dei risultati dell'intercettazione) nei termini fissati dalla giurisprudenza di legittimità[75]. Peraltro, «in fase di indagini preliminari, non è necessario che nel provvedimento che utilizza, ai sensi dell'art. 270 c.p.p., i risultati di intercettazioni effettuate in procedimento diverso sia espressamente motivata l'indispensabilità di tali risultati ai fini dell'accertamento dei delitti per cui si procede e per i quali è previsto l'arresto in flagranza, potendo la valutazione di indispensabilità essere compiuta anche implicitamente, mediante l'attribuzione agli elementi utilizzati di specifica rilevanza ai fini della decisione adottata»[76].

Di rilievo i riflessi di tale inquadramento sulla **utilizzabilità di dette prove**.

Al riguardo, è stato affermato che possono essere utilizzate in un **procedimento italiano** le intercettazioni disposte in procedimenti penali svoltisi all'estero, acquisite per rogatoria dall'autorità giudiziaria italiana, **purché** siano rispettate le **condizioni eventualmente poste dall'autorità estera** all'utilizzabilità degli atti richiesti **e sempre che le intercettazioni** stesse siano avvenute nel **rispetto delle regole formali e sostanziali** che le disciplinano e altresì nel rispetto dei **fondamentali principi di garanzia**, aventi rilievo di ordine costituzionale, propri del nostro ordinamento.

Ciò apre a nuovi corollari e ulteriori problematiche.

Secondo una **prospettiva ermeneutica più radicale,** si è affermato che la **necessità per il Giudice nazionale di effettuare una verifica giudiziale di utilizzabilità degli atti probatori "importati"** - sempre con riferimento alla vicenda delle comunicazioni acquisite sulla piattaforma "Sky ECC" - «**è in tal caso ultronea, perché non prevista dall'art. 270 cod. proc. pen. neppure per il trasferimento di intercettazioni nei procedimenti interni**»[77].

La questione pare più complessa. Salva l'esigenza di un controllo giurisdizionale attivabile dall'interessato nello Stato di esecuzione, in ossequio al "principio di equivalenza", non sembra si possa omettere di verificare **se l'attività di utilizzo del trojan da parte dell'A.G. francese non contrasti con i principi generali del nostro codice di rito che disciplinano l'ambito di utilizzo di detto strumento di captazione delle comunicazioni**. L'esigenza di valutare l'utilizzabilità degli esiti dell'attività di intercettazione condotta dalla Autorità francese deriva dalla previsione, contenuta nell'art. **14, par. 7, della Direttiva**, in base al quale "lo Stato di emissione tiene conto del fatto che il riconoscimento o l'esecuzione di un OEI sono stati impugnati con successo conformemente al proprio diritto nazionale. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'OEI". Sul punto, sempre in riferimento alla acquisizione delle chat, si è affermato che, mentre la questione relativa alla illegittima emissione dell'OEI da parte del pubblico ministero italiano non può essere dedotta dinanzi al giudice italiano,

[75] Ai sensi dell'art. 1 del DL. 10/08/2023, n. 105 (convertito in legge il 9 ottobre 2023, n. 137), commi «2-*quater*. All'articolo 270, comma 1, del codice di procedura penale, le parole: «e dei reati di cui all'articolo 266, comma 1» sono soppresse. 2-*quinquies*. La disposizione di cui al comma 2-*quater* si applica ai procedimenti iscritti successivamente alla data di entrata in vigore della legge di conversione del presente decreto. Ciò rende plausibile un ritorno alla vigenza dell'insegnamento della Sezioni Unite Cavallo (sentenza n. 51/2020) per i procedimenti iscritti da quest'ultima data.

[76] Cass., Sez. III, n. 5821 del 18/01/2022, Napolitano, Rv. 282804 – 01.

[77] Così, Cass., Sez. VI, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363- 02.

nel caso in cui tale ordine sia stato emesso per acquisire una prova già disponibile nello Stato di esecuzione e la stessa sia stata definitivamente trasmessa da detto Stato, la difesa può invece far valere la **mancanza delle condizioni di ammissibilità della prova secondo l'ordinamento processuale italiano**[78]. Ove si condivida tale conclusione, la correlata valutazione andrebbe condotta alla luce della previsione di cui all'**art. 271, comma l, c.p.p.** (valutazione che, **su eccezione di parte**, compete anche al Giudice del procedimento nel quale vengono acquisite le intercettazioni eseguite in diverso procedimento: *arg*. *ex* Sez. U, n. 45189 dell7/11/2004, Esposito, Rv. 229245- 01)[79]. In definitiva, muovendo da tale opzione ermeneutica, e ferma restando la legittimità della emissione dell'OEI da parte della competente Autorità giudiziaria italiana e della conseguente trasmissione dei relativi atti di indagine da parte dell'Autorità estera, viene profilandosi, sulla base del ricordato assetto normativo - che specificamente governa le modalità di funzionamento dell'OEI (necessità, proporzionalità ed equivalenza dell'atto di indagine specificamente oggetto di richiesta) e, più in generale, dei pertinenti principi costituzionali (artt. 15, 24 e 111) e convenzionali (art. 8 Conv. EDU) - un'opzione esegetica favorevole ad assicurare la possibilità di attivare un **effettivo controllo giurisdizionale, quantomeno successivo**, sul contenuto delle acquisizioni probatorie da altro Stato UE.

Del resto, che la materia in esame coinvolga **fondamentali principi di garanzia**, aventi rilievo di ordine costituzionale, propri del nostro ordinamento, lo avvalorano molti elementi e approdi giurisprudenziali. In tema di utilizzo di dati probatori derivanti da intercettazioni effettuate in altro procedimento, le **Sezioni Unite Cavallo** (sent. n. 51/2020, Rv. 277395 - 01) hanno precisato come l'art. 15 Cost tuteli due distinti interessi, «quello inerente alla libertà ed alla segretezza delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale (Corte cost., sent. n. 34 del 1973)», aggiungendo che «il diritto a una comunicazione libera e segreta è inviolabile, nel senso generale che il suo contenuto essenziale non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal Costituente», mentre, in base all'art. 15 Cost., «lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato dell'autorità giudiziaria» (Corte cost., sent. n. 366 del 1991). Peraltro la sentenza ha riconosciuto come «l'esigenza di repressione dei reati corrisponde a un interesse pubblico primario, costituzionalmente

[78] Cass., Sez. VI, n. 44155 del 26/10/2023, Kolgjokaj Indrit, Rv. 285362 – 02.

[79] Sulla base di tale orientamento, ancora, si è affermato, nell'ipotesi di utilizzo di intercettazioni disposte in altro procedimento, che «In tema di misure cautelari personali, nel caso in cui l'ordinanza che dispone la misura cautelare sia fondata anche sulle risultanze di intercettazioni disposte nell'ambito di un procedimento dal quale siano stati separati taluni reati per ragioni di competenza territoriale, il tribunale del riesame, nel giudizio "ad quem", è tenuto a procedere ad una autonoma valutazione circa la sussistenza dei presupposti e delle condizioni di legittimità delle operazioni di intercettazione disposte nel procedimento originario prima della separazione, sempreché la consistenza delle stesse intercettazioni sulla quale si fonda il provvedimento impugnato sia stata radicalmente posta in discussione con la formulazione di eccezioni non pretestuose e seriamente prospettate» (Sez. 6, n. 36874 del 13/06/2017, Romeo, Rv. 270812 - 01). In detta pronuncia si è evidenziato che «Deve altresì rilevarsi, alla luce dei principi stabiliti da questa Corte (Sez. l, in particolare, n. 42006 del 28/10/2010, Tavelli, Rv. 249109), che le valutazioni circa l'utilizzabilità del materiale proveniente da intercettazioni effettuate nel procedimento in cui sono state disposte le relative operazioni non vincolano il Giudice del diverso procedimento, che conserva, dunque, piena autonomia decisoria e in tal senso deve procedere ad autonomo apprezzamento. Non è possibile, dunque, ritenerne la tralaticia utilizzabilità solo per il fatto che l'intercettazione disposta nell'uno sia stata utilizzata nell'altro in presenza delle condizioni di cui all'art. 270 cod. proc. pen., poiché nel secondo procedimento il Giudice, quand'anche venga sollecitato ad operare il suo vaglio delibativo in sede incidentale, deve rivendicare la propria autonomia di valutazione, essendo diversa la res iudicanda caratterizzata dal diverso fatto di reato, anche se contestato a carico degli stessi soggetti comuni ai due procedimenti».

rilevante, il cui soddisfacimento è assolutamente inderogabile», interesse che giustifica «anche il ricorso a un mezzo dotato di formidabile capacità intrusiva, quale l'intercettazione telefonica»; d'altra parte, «le restrizioni alla libertà e alla segretezza delle comunicazioni conseguenti alle intercettazioni telefoniche sono sottoposte a condizioni di validità particolarmente rigorose, commisurate alla natura indubbiamente eccezionale dei limiti apponibili a un diritto personale di carattere inviolabile, quale la libertà e la segretezza delle comunicazioni» (Corte cost., sent. n. 366 del 1991)». Sempre in relazione alla necessità di bilanciare la tutela della riservatezza delle comunicazioni e la salvaguardia dei dati personali con le esigenze di repressione dei reati si è pronunciata, inoltre, la **Corte di Giustizia dell'Unione Europea** nella nota decisione "**Prokuratuur**" (Grande Sezione, sentenza del 2 marzo 2021, nella causa C-746/18, avente ad oggetto la domanda di pronuncia pregiudiziale proposta dalla Corte suprema dell'Estonia con decisione del 12 novembre 2018). Al riguardo (punto 35) la Corte UE - che si è espressa in merito all'interpretazione dell'art. 15, par. l, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, sul trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche - pur pronunciandosi in riferimento a un diverso genere di prove elettroniche e non riferibile, direttamente o indirettamente, all'acquisizione dei dati presso la piattaforma Sky-ECC per delitti di criminalità organizzata, traffico internazionale di stupefacenti o riciclaggio[80], ha stabilito, in linea generale, che «soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono atti a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo e tali da permettere di trarre precise conclusioni sulla vita privata delle persone interessate (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 54)». La sentenza in oggetto ha precisato, però (punto 45), che «l'articolo 15, paragrafo l, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo l, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle 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». Va altresì evidenziato che l'esigenza di una particolare protezione della riservatezza dei dati personali emerge finanche dalle previsioni contenute nell'**art. 3 d.lgs. 108/2017**, cit., che, dando attuazione a quanto contenuto nell'art. 20 della direttiva 2014/41/UE, stabilisce quanto segue: «Nel compimento delle attività relative all'emissione, alla trasmissione, al riconoscimento ed all'esecuzione dell'ordine di indagine, i dati personali sono trattati secondo le disposizioni legislative che regolano il trattamento dei dati giudiziari e in conformità agli atti normativi dell'Unione europea e alle Convenzioni del Consiglio d'Europa». Tema, questo, che si correla anche alla tutela del "domicilio informatico", la cui protezione da abusive ingerenze esterne può trovare, secondo parte della dottrina, un solido riferimento costituzionale nell'art. 14 Cost. E sempre la **Corte di Giustizia**, con la sentenza **emessa il 21 dicembre 2023 nella causa C-281/22 - G. K. e altri**, ha avuto modo di delimitare, in relazione alle indagini svolte dalla Procura Europea in più Stati membri, ma con un espresso riferimento anche alla disciplina che regola l'OEI, gli ambiti di verifica rispettivamente spettanti alle diverse Autorità coinvolte nel procedimento di raccolta transnazionale delle prove[81]. La predetta sentenza ha altresì

[80] Sul punto, v. Cass. Sez. VI, n. 46833 del 26/10/2023, Bruzzaniti, cit.

[81] In particolare, al punto 63 si è precisato che «Dal combinato disposto degli articoli 6 e 9 di tale direttiva [n. 2014/41] risulta che il sistema di cooperazione giudiziaria ivi previsto si basa, come quello istituito dalla decisione quadro

chiarito, nelle conclusioni, che il controllo giurisdizionale sulle misure investigative in altri Stati membri può vertere solo sugli elementi relativi all'esecuzione di tali misure; tuttavia, «nel caso di misure investigative che comportino ingerenze gravi nei diritti fondamentali, quali le perquisizioni, lo Stato membro cui appartiene il PED incaricato del caso deve prevedere nel diritto nazionale garanzie adeguate e sufficienti, quali un controllo giurisdizionale preventivo, per assicurare la legittimità e la necessità di tali misure».

In caso di "importazione" a seguito di OEI degli esiti delle intercettazioni eseguite dall'Autorità giudiziaria francese, ove si ritenesse applicabile l'orientamento secondo cui in tale ipotesi è comunque necessario un controllo da parte della Autorità giudiziaria italiana, sarebbe necessario anche valutare, nei limiti di quanto stabilito dalla richiamata Direttiva, se nell'ordinamento interno sia **legittimo disporre ed effettuare il suindicato complesso sistema di acquisizione delle chiavi di decrittaggio nell'ambito della intercettazione effettuata su un *server* di una piattaforma informatica**.

In altri termini ferma restando la legittimità dell'attività di intercettazione delle comunicazioni svolta all'estero, ci si dovrebbe interrogare circa la possibilità, nel nostro ordinamento, di utilizzare il ***trojan***, non solo per disporre un'intercettazione, ma anche per acquisire - attraverso il sistema sopra descritto - le **chiavi di decrittaggio**. Attività, quest'ultima, che potrebbe confrontarsi con le condizioni di legittimità di una "prova atipica" *ex* **art. 189 c.p.p**., nel caso in esame non consentita ove ritenuta non rispondente ai canoni dell'art. 15 della Carta fondamentale. L'aspetto relativo all'utilizzo del trojan per acquisire le chiavi di decrittaggio non risulta essere stato affrontato dalla giurisprudenza[82]. La S.C. ha affermato il principio secondo cui le prove "atipiche" acquisite in violazione di un divieto derivante da principi costituzionali sono illecite e quindi inutilizzabili (Sez. U, n. 26795 del 28/03/2006, Prisco, Rv. 234270- 01). Per l'acquisizione delle chiavi di cifratura depositate presso i criptofonini, una delle strade plausibili è quella di ritenere che dal *server* infettato si sia fatta partire una notifica *push*; attività questa potrebbe ritenersi acquisizione probatoria illegittima perché lesiva della libertà morale dei soggetti coinvolti[83]. Si oppone, però, che, qui a collaborare involontariamente con gli investigatori non è tanto l'utente del servizio, che infatti non è neppure chiamato a scaricare il messaggio di notifica, ma piuttosto è il criptofonino stesso che, interfacciandosi con il *server*, disvela automaticamente le proprie chiavi di cifratura. Ciò però rende maggior forza alle ragioni di chi ritiene che, in funzione del rispetto del diritto di difesa, l'algoritmo impiegato per decrittare i flussi comunicativi captati o comunque sequestrati all'interno del *server* debba essere messo senz'altro a disposizione delle parti unitamente alle stringhe informatiche non ancora decriptate[84]. Restando in tema, ove si ritenga che l'utilizzo del captatore informatico sia

2002/584, su una ripartizione delle competenze tra l'autorità giudiziaria emittente e l'autorità giudiziaria dell'esecuzione, nel cui contesto spetta all'autorità giudiziaria emittente verificare il rispetto delle condizioni sostanziali richieste per l'emissione di un ordine di indagine europeo, senza che tale valutazione possa, secondo il principio del mutuo riconoscimento, essere successivamente riesaminata dall'autorità giudiziaria dell'esecuzione», aggiungendo, al punto 74, che «La suddivisione di responsabilità descritta ai punti 71 e 72 della presente sentenza lascia quindi impregiudicati gli obblighi discendenti dal rispetto dei diritti fondamentali nell'adozione di misure investigative assegnate che, come quelle oggetto del procedimento principale, costituiscono ingerenze nel diritto di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni, sancito all'articolo 7 della Carta, nonché nel diritto di proprietà consacrato all'articolo 17 della stessa».

[82] I precedenti relativi ad intercettazioni effettuate su cellulari "blackberry", di cui si darà conto infra, differiscono dalla situazione in esame perché per essi la società gestrice forniva, su richiesta della Autorità giudiziaria, le comunicazioni decrittate.

[83] L. FILIPPI, *Criptofonini e diritto di difesa*, in *https://www.penaledp.it/criptofonini-e-diritto-di-difesa*, 23 giugno 2023.

[84] L. LUDOVICI, *op. cit*., pp. 422-423 il quale chiosa: «In assenza di questi dati, infatti, non si vede come sia possibile esercitare a pieno il diritto di difesa su un tema di fondamentale importanza qual è quello della piena corrispondenza tra il testo originario (i.e., la stringa informatica) e il testo intellegibile introdotto come prova nel giudizio. Senza contare che, quando i flussi comunicativi siano stati acquisiti tramite captazioni live, la transizione dei dati telematici dal linguaggio binario delle stringhe ad un linguaggio intellegibile, non integrando certo una operazione irripetibile, sembra destinata a trovare ingresso nel fascicolo dibattimentale non certo sotto forma di brogliaccio di p.g. ma necessariamente con le forme garantite e, di regola, ineludibili della perizia».

consentito, nel nostro ordinamento, per effettuare "l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi" (art. 266-*bis* c.p.p.), può sostenersi che l'attività di **inoculazione del virus informatico, anche funzionale ad acquisire le chiavi di decrittaggio** (trasmesse dai "criptofonini" a ciò indotti dal "*malware*"), si collochi comunque all'interno di un'attività "intercettativa" di un flusso di comunicazioni informatiche. Va rilevato che tale conclusione è resa parzialmente problematica dal fatto che l'utilizzo del captatore informatico è autorizzato – in termini letterali - soltanto per l'inserimento su un "dispositivo elettronico portatile"[85]. Se la legittimità dell'utilizzo del captatore informatico nel caso di specie sia comunque ritenuta condivisibile, deve poi rilevarsi come, nella medesima prospettiva, sia stata ritenuta «legittima, ove ricorrono i presupposti di legge per l'autorizzazione, la disposizione di un successivo decreto di intercettazione sul medesimo bersaglio o dispositivo elettronico già colpito da attività investigativa, giustificata dalla necessità di far ricorso, per ragioni d'indagine, allo strumento più pervasivo del "captatore informatico", configurandosi in tal caso un nuovo ed autonomo mezzo di ricerca della prova che non presenta interferenze con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari di captazione»[86]. Inoltre, ove l'ingresso nel *server* sia stato effettuato senza l'assenso della società che lo gestiva ma attraverso l'impiego di un *malware*, si pone il problema di verificare la legittimità di tale operato. Infatti, la situazione di un *server* occultamente penetrato potrebbe condurre a considerare l'intrusione quale perquisizione informatica clandestina e dunque illegittima se svolta senza le garanzie previste dalla legge. Considerando la memoria del *server* un domicilio informatico di ciascun utente relativamente ai dati digitali che lo riguardano, la categoria della prova atipica potrebbe rivelarsi di difficoltosa praticabilità, non potendo comprimere valori che, al contrario, sono presidiati dalla riserva di legge, come il domicilio, compreso quello informatico[87]. In ogni caso l'utilizzabilità dei dati acquisiti in forza del successivo sequestro potrebbe conservarsi, per il noto principio – che a tutt'oggi, se non altro a livello giurisprudenziale, gode di ottima salute - del *male captum bene retentum*[88].

V'è altresì da considerare che, ai fini dell'impiego del captatore informatico, il nostro ordinamento, a seguito della recente interpolazione del testo dell'art. 267, comma 1, c.p.p. (intervenuta per effetto dell'art. 1, comma 2-*bis*, d.l. 10 agosto 2023, n. 105, conv. nella l. 9 ottobre 2023, n. 137), impone all'autorità giudiziaria l'assolvimento di un rigoroso **onere motivazionale** non solo nella indicazione delle specifiche ragioni che ne giustificano l'attivazione, ma anche nella esposizione di una **autonoma valutazione della necessità, "in concreto", del ricorso a tale peculiare modalità tecnica di espletamento del relativo mezzo di ricerca della prova**. Una motivazione, dunque, "rafforzata", attraverso la quale il Giudice è chiamato, nel rispetto del canone di proporzionalità, a spiegare le ragioni poste a fondamento dell'utilizzo di uno strumento di indagine particolarmente invasivo della riservatezza delle persone, dando conto, in concreto, del bilanciamento da lui operato tra i diversi beni di rilievo costituzionale confliggenti nel caso di specie.

Altri profili problematici si correlano, infine, anche all'**utilizzabilità a fini probatori degli atti compiuti dall'Autorità estera e importati nel nostro ordinamento a mezzo di OEI**. Infatti, l'**art. 36 d.lgs. cit.** stabilisce al comma 1 che "Sono raccolti nel fascicolo per il dibattimento di cui all'articolo 431 del codice di procedura penale: a) i documenti acquisiti all'estero mediante ordine di indagine e i verbali degli atti non ripetibili assunti con le stesse modalità; b) i verbali degli atti, diversi da quelli previsti dalla lettera a), assunti all'estero a seguito di ordine di indagine ai quali i difensori sono stati posti in grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana".

[85] In argomento, cfr. artt. 266, commi 2 e 2-*bis*, 267, commi 1 e 2-*bis*, 89 disp. att. c.p.p.; v. anche Sez. U., n. 26889 del 28/04/2016, Scurato, Rv. 266905 – 01.

[86] Cass., Sez. V, n. 32426 del 24/09/2020, Guadadiello, Rv. 279779 - 01.

[87] Sul punto, P. BRONZO, *L'impiego del trojan horse informatico nelle indagini penali, in Rivista italiana per le scienze giuridiche*, 8/2017, 348.

[88] Per l'affermazione del principio, si v. Cass., Sez. Un., 16 maggio 1996, Sala, in Cass. pen., 1996, 3268 ss. Per una ricostruzione critica cfr. F. R. DINACCI, *L'inutilizzabilità e il male captum bene retentum: vecchie superstizioni e nuove consapevolezze*, in Archivio Penale 2023, n. 2.

Sulla base di detta disciplina (analoga a quella contenuta nell'art. 431 cit.) potrebbe comunque ritenersi che il mancato inserimento negli atti del procedimento dei diversi **provvedimenti autorizzatori adottati dall'Autorità francese** non rilevi atteso che «In tema di intercettazioni, i decreti autorizzativi non rientrano tra gli atti che devono essere inseriti nel fascicolo per il dibattimento *ex* art. 431, primo comma, cod. proc. pen., sicché il loro mancato inserimento nello stesso non determina alcuna inutilizzabilità degli esiti delle attività di captazione, salvo che non sia prospettata l'inesistenza o la nullità degli stessi» (Sez. l, n. 7485 del 21/01/2015, PG in proc. Gentile, Rv. 262S33 - 01).

4. Garanzie difensive interne per l'importazione delle comunicazioni decrittate nel procedimento estero e acquisite a seguito di OEI.

4.1. I principi di proporzionalità e di equivalenza secondo l'ordinamento interno: le attività di indagine governate da tali regole.

L'art. l, par. l, della **Direttiva 2014/41UE** consente il ricorso all'OEI anche per acquisire prove che già sono in possesso delle competenti Autorità dello Stato di esecuzione[89]. L'art. 6, **par. l**, **della citata Direttiva** stabilisce, inoltre, che «L'autorità di emissione può emettere un OEI solamente quando ritiene soddisfatte le seguenti **condizioni**: a) l'emissione dell'OEI è necessaria e **proporzionata** ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata (cd. profilo di proporzionalità); e b) l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere **emessi alle stesse condizioni in un caso interno analogo**» (cd. **profilo di equivalenza**). L'art. 6, par. 2, cit. stabilisce che «Le condizioni di cui al paragrafo l sono valutate dall'autorità di emissione per ogni caso». Ne consegue: a) che **l'ambito di applicazione della direttiva si estende anche agli atti investigativi con i quali si richiede il trasferimento di prove già esistenti**; b) che l'art. **6, par. l, lett. b), della direttiva può applicarsi anche a un ordine investigativo europeo emesso ai fini del trasferimento di prove già esistenti nell'ordinamento richiesto**, come sembrerebbe verificatosi nella più parte dei casi di specie; c) che il riferimento ad "un caso interno analogo" di cui all'art. 6, par. l, lett. b), della citata direttiva impone all'autorità di emissione, anche nell'ipotesi che un ordine di indagine europeo sia finalizzato al trasferimento di prove già in possesso dello Stato di esecuzione, di valutare se e a quali condizioni il proprio ordinamento consenta l'importazione di prove raccolte mediante l'intercettazione di comunicazioni tra procedimenti penali a livello interno. La connessa disposizione di cui all'**art. 14, par. 2**, della direttiva consente di **contestare e vagliare il mancato rispetto di tali presupposti e condizioni esclusivamente dinanzi alle autorità dello Stato di emissione**.

Nell'**ordinamento italiano** l'assetto delineato dal legislatore europeo ha ricevuto la sua conforme attuazione attraverso le correlate disposizioni di cui agli **artt. 2, comma l, lett. a), 9, comma 5, lett. a), 10, comma l, 12, comma l, d.lgs. 108/2017**.

Il "**principio di proporzione**" è declinato a livello interno dall'**art. 7 d.lgs. cit**., che stabilisce nel comma che «L'ordine di indagine non è proporzionato se dalla sua esecuzione può derivare un sacrificio ai diritti e alle libertà dell'imputato o della persona sottoposta alle indagini o di altre persone coinvolte dal compimento degli atti richiesti, non giustificato dalle esigenze investigative o probatorie del caso concreto, tenuto conto della gravità dei reati per i quali si procede e della pena per essi prevista». Sia in sede di esecuzione ("procedura passiva") che in sede di emissione ("procedura attiva") dell'OEI l'A.G. non è chiamata a svolgere un ruolo meramente passivo, ma **deve esercitare il suo sindacato sull'atto richiesto anche attraverso il test di proporzionalità** (*ex* artt. 7 d.lgs. cit.

[89] Nel settimo considerando della direttiva 2014/41/UE chiarisce, infatti, che «L'OEI deve essere emesso affinché nello Stato che lo esegue (lo «Stato di esecuzione») siano compiuti uno o più atti di indagine specifici ai fini all'acquisizione di prove. Ciò include anche l'acquisizione di prove già in possesso dell'autorità di esecuzione».

e 6, comma l, lett. a), direttiva cit.), ad eccezione delle **specifiche ipotesi previste dall'art. 9, comma 5, d.lgs**. cit., ove, ferme le condizioni ostative in linea generale contemplate nell'art. **10, comma l, d. lgs. cit.** (tra le quali figura anche il necessario vaglio di compatibilità dell'atto richiesto con gli obblighi previsti dall'art. 6 TUE e dalla Carta dei diritti fondamentali dell'Unione europea), il legislatore ha stabilito che "si provvede in ogni caso all'esecuzione" per determinate categorie di atti d'indagine o di assunzione della prova (acquisizione dei verbali di prove di altro procedimento e di informazioni contenute in banche dati accessibili all'autorità giudiziaria, atti d'indagine privi di incidenza sulla libertà personale, audizioni di testimoni o consulenti, dell'imputato o dell'indagato ecc.)[90]. Il **principio di proporzionalità** impone che **l'attività da compiere debba essere adeguata e funzionale sia rispetto al suo presupposto** (il reato), **sia rispetto all'obiettivo che intende perseguire** («le esigenze investigative o probatorie»), in modo che la sua esecuzione comporti il minor sacrificio possibile per i diritti e le libertà dell'imputato o dell'indagato[91]. Così, il "trasferimento" in Italia delle comunicazioni relative agli indagati sembra doversi ritenere "proporzionato" in riferimento al titolo di reato e al grado della risposta sanzionatoria (si pensi all'art. 74 d.P.R. n. 309 del 1990), risultando rispettata, sotto tale profilo, la lett. a) dell'art. 6, par. l, della direttiva. Ciò rende evidente la necessità di interrogarsi, all'interno dell'ordinamento dello Stato emittente, sia in relazione al grado di interferenza e compressione nell'esercizio dei diritti fondamentali coinvolti, sia in ordine al profilo, strettamente connesso, delle specifiche modalità processuali con le quali sarebbe stato possibile acquisire in Italia i contenuti delle predette conversazioni (lett. b).

4.2. Il principio di equivalenza e la legittimità della decriptazione realizzata captando chiavi crittografiche.

Sul punto, oltre a quanto si è osservato al par. 3.5., andrebbero anche verificati gli effetti della "**asimmetria**" rilevabile tra le previsioni del d**.lgs. n. 108/2017**, che sembrano consentire **l'intercettazione**, anche a mezzo di *trojan*, non solo di un dispositivo, ma anche di interi "sistemi informatici o telematici" (v. artt. 24 e 43) e la disciplina interna, ove tale ultima modalità di indagine non sembra invece trovare un'espressa disciplina (gli artt. 266, commi 2 e 2-*bis*, c.p., p. e 89, comma 2, disp. att. c.p.p. si riferiscono all'inserimento del captatore informatico su un "dispositivo elettronico portatile"). Né, peraltro, può omettersi di rilevare che nel caso in esame l'utilizzo del *trojan* non sembrerebbe esser stato finalizzato solo ad effettuare l'intercettazione dei dati comunicativi, quanto piuttosto a consentire, attraverso il meccanismo descritto, l'acquisizione delle loro chiavi di decrittaggio. Ora alla riflessione più attenta non sembra problematico che la disciplina concerna l'utilizzo del captatore solo come strumento di intercettazione ambientale da installarsi su dispositivi portatili e non anche su dispositivi fissi, come il *server*. Infatti, in quest'ultima fattispecie, l'utilizzo del captatore informatico non pone in pericolo la violazione indiscriminata della riservatezza del domicilio, in quanto sono captati i flussi comunicativi scambiati tra due dispositivi portatili e non le conversazioni tra presenti; ragion per cui il captatore informatico sembrerebbe sottrarsi alla speciale disciplina di cui all'art. 266, c. 2-*bis* c.p.p. – non generando quei rischi che la stessa è preordinata a scongiurare [92] – per ricadere nella sfera applicativa della **normativa di carattere generale**.

Sotto il profilo dell'equivalenza (ove non la si voglia ricondurre a quello della proporzione), la possibile criticità di tale tipologia di ricerca della prova riguarda **l'ampiezza della captazione**: a fronte di un *server* "bucato", la captazione riguarderà non solo le comunicazioni e le conversazioni ritenute potenzialmente rilevanti nel procedimento ove l'intercettazione sia stata disposta, ma anche tutti i flussi comunicativi intercorsi tra gli abbonati al servizio, acquisendo materiale probatorio ottenuto attraverso il monitoraggio di una moltitudine di utenze di cui, nel provvedimento

[90] Cass., Sez. VI, n. 8320 del 31/01/2019, Creo, Rv. 275732.
[91] Cass., Sez. VI, n. 8320/2019, cit.
[92] Cass., Sez. Un., 28 aprile 2016, Scurato, Rv. 266905-01.

autorizzativo, non era però stata fatta alcuna menzione e rispetto alle quali, non era stato compiuto il doveroso vaglio circa la necessità di sacrificarne la riservatezza. Ebbene, almeno fino a quando, sul piano tecnico, non risulti limitabile il controllo occulto ai soli flussi comunicativi di interesse per il procedimento in corso, tale modalità di indagine vivrà opposte letture di adattamento all'ordinamento interno. Se, infatti, la legge consente di violare la riservatezza di quelle comunicazioni rispetto alle quali sussistono determinati presupposti giustificativi, si dubita della legittimità di autorizzare un'attività di intercettazione (telematica) a tappeto di tutti i flussi comunicativi veicolati dal *server* infettato[93].

Tali questioni rendono ragione della rilevanza della questione rimessa alle Sezioni Unite, richieste di chiarire se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'Autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul "*server*" di una piattaforma criptata sia soggetta nell'ordinamento interno ad un controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità dei dati raccolti.

4.3. Il contraddittorio sul processo di formazione della prova e il diritto della difesa di accesso all'algoritmo di decriptazione e agli originali messaggi criptati.

Uno dei profili sovente più discussi quale condizione di utilizzabilità delle prove "aliene" acquisite nel nostro ordinamento attiene al diritto della **difesa di disporre, a richiesta, dell'algoritmo per la decrittazione delle "chat".** Occorre premettere che tale algoritmo non è stato comunicato neppure all'A.G. italiana che ha ricevuto solo le conversazioni già tradotte "in chiaro".

Sul punto, in riferimento alle intercettazioni effettuate su un dispositivo cellulare Blackberry (con caratteristiche assimilabili ai "criptofonini", con la particolarità che, a differenza di Sky Global, la società produttrice e gestrice del sistema Blackberry forniva alla A.G. le chat decrittate) la giurisprudenza di legittimità aveva maturato un contrasto, poi rifluito in alcune pronunce relative alle chat intercorse su SkyEcc. Secondo un primo orientamento, ove l'attività di messa in chiaro di messaggi criptati scambiati mediante sistema Blackberry sia stata svolta dal fornitore del servizio fuori dal contraddittorio, la difesa ha diritto di ottenere, oltre alla versione originale e criptata dei messaggi, anche le chiavi di sicurezza necessarie alla decriptazione, a pena di nullità *ex* art. 178, lett. c), c.p.p. sanabile dall'istanza di giudizio di abbreviato[94]; in particolare, «laddove alla difesa - non solo in sede cautelare, ma anche nel corso del giudizio di merito - fosse precluso di prendere cognizione dei flussi di comunicazioni informatiche o telematiche, nella loro versione originale ed integrale, e fosse conseguentemente impedito l'esercizio di ogni potere di controllo, sussisterebbe una nullità di ordine generale a regime intermedio, derivante dalla violazione della disciplina diretta ad assicurare l'assistenza e la rappresentanza dell'imputato in una ipotesi in cui, tuttavia, non è obbligatoria la presenza del suo difensore». Nello stesso senso si è più di recente pronunciata la Cassazione, con riferimento all'acquisizione, tramite OEI, e all'utilizzo in fase cautelare delle comunicazioni intercorse su SkyEcc. Affrontando il tema della utilizzabilità processuale, anche in sede cautelare, della **messaggistica acquisita da Europol**, tramite il coordinamento delle attività delle polizie francese, belga e olandese, attraverso l'accesso ai *server* di SkyEcc che la conservavano in memoria, la Corte di legittimità ha ritenuto non sufficiente la formale acquisizione della messaggistica tramite OEI, richiedendo il riscontro di conoscenza delle **modalità di acquisizione del detto materiale.** Sarebbe necessario valutare, in particolare, nell'ambito del procedimento interno, che tali modalità di acquisizione della messaggistica non siano in contrasto con norme inderogabili e principi fondamentali del nostro ordinamento. Ciò proprio in nome del principio del contraddittorio che implica che la dialettica procedimentale debba esplicarsi non soltanto relativamente al vaglio del

[93] In senso sostanzialmente conforme, SIRACUSA, *Il Giano bifronte: autorità e libertà nella data retention. A proposito di una recente pronuncia della Corte di cassazione*, in Arch. Pen., 2023, 2, 9.
[94] Cass. Sez. IV, n. 49896 del S/10/2019, P.G. c. Brandimarte, Rv. 277949- 03.

materiale acquisito, ma si deve estendere anche alle modalità di acquisizione dello stesso. Ciò è funzionale al controllo della legittimità del procedimento acquisitivo, anche nell'ottica delineata dall'art. 191 del c.p.p., il quale stabilisce l'inutilizzabilità delle prove acquisite in violazione dei divieti stabiliti dalla legge. La Cassazione ha dunque statuito che «le modalità di acquisizione del materiale probatorio rilevano, inoltre, nell'ottica della valutazione della valenza epistemica di quest'ultimo, sotto il profilo, per quanto inerisce alla specifica problematica *sub iudice*, 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**, ragione per cui la problematica in disamina dispiega la propria rilevanza anche relativamente alla fase della captazione e della decrittazione dei flussi telematici. Tutto ciò comporta imprescindibilmente la possibilità di conoscere le modalità di svolgimento dell'attività investigativa svolta e il procedimento di acquisizione di tale messaggistica, onde consentire la piena esplicazione del diritto di difesa, attraverso l'instaurazione di una proficua dialettica procedimentale in ordine ad ogni profilo di ritualità, rilevanza, attendibilità e valenza dimostrativa che possa venire in rilievo, nell'ottica dell'imputazione. Ciò che nel caso in esame non è stato consentito ai difensori»[95].

Tale interpretazione potrebbe trovare un supporto ove si riconoscesse sussistere il **diritto di accesso della difesa alla versione originale dei messaggi oggetto di decrittazione**, ancorandolo alle particolari garanzie riconosciute, anche in ambito processuale, dall'**art. 8 del d.lgs. 51 del 2018** (di recepimento della direttiva 2016/680) rispetto ai processi decisionali algoritmici (qual è quello sotteso alla decrittazione, appunto algoritmica, dei messaggi). In particolare, la citata disposizione stabilisce che «sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge (comma 1). Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento (comma 2)». D'altro canto, la fondamentale esigenza di garantire la genuinità e la corretta conservazione dei dati acquisiti è ribadita anche dalla previsione del **decreto interministeriale del 6 ottobre 2022**, in tema di individuazione delle prestazioni funzionali alle operazioni di intercettazione e per la determinazione delle relative tariffe, adottato ai sensi della legge n. 103 del 2017, che, all'art. 3, comma 2, lett. c), impone ai fornitori delle prestazioni «la tempestiva trasmissione e consegna, mediante canali cifrati che ne assicurano la segretezza, dei contenuti eventualmente acquisti anche diversi da quelli conseguenti all'esecuzione delle prestazioni obbligatorie, secondo procedure informatiche approvate dal Ministero della Giustizia, in grado di assicurare all'Autorità giudiziaria l'originalità, l'integrità e la fruibilità dei dati trasmessi e/o ricevuti dall'identità di rete». Sul tema va anche richiamata, per i profili di carattere generale, la recente sentenza della Corte EDU (Grande Camera), 26 settembre 2023, Yuksel Yalçinkaya c. Turchia, n. 15669/20, che ha affermato che «Sussiste la violazione degli artt. 6, par. l, 7 e 11 della CEDU in relazione ad una condanna per appartenenza ad una organizzazione terroristica che sia stata emessa all'esito di un processo nel quale non sono state assicurate all'imputato adeguate garanzie procedurali volte a controbilanciare la limitazione del diritto della difesa all'astensione dei dati "grezzi" delle comunicazioni crittografate scambiate sulla piattaforma "Bylock"». Al riguardo si è osservato che, in base a detta pronuncia, «il diritto ad un processo in contraddittorio presuppone quindi che l'autorità inquirente riveli alla difesa tutte le prove, anche quelle "elettroniche" e non solo quelle che l'accusa ritiene rilevanti. Tale diritto non è, tuttavia, assoluto potendo rendersi necessario un suo bilanciamento con interessi concorrenti, quali la sicurezza nazionale o la necessità di mantenere segreti i metodi di indagine dei reati da parte della polizia»[96]. Secondo una diversa lettura delle implicazioni sottese alla richiamata decisione della Corte EDU «detta pronuncia, pur affrontando il tema del rispetto del diritto di difesa in indagini basate sull'utilizzazione di piattaforme di messaggeria criptate, riguarda un caso del tutto eccentrico rispetto

[95] Cass. Sez. IV, n. 32915 del 15/07/2022, Lori, n.m.
[96] Cass. Sez. VI, n. 44154 del 26/10/2023, Iaria, Rv. 285284 – 01.

a quello francese, perché descrive la violazione dei basilari fondamenti dello Stato di diritto e dell'equo processo da parte dell'Autorità giudiziaria turca, già condannata dalla stessa Corte EDU per gli arresti anche di magistrati e avvocati avvenuti in base ai soli messaggi scambiati tra terzi sull'applicativo ByLock, in nessun modo prospettabili con riferimento allo Stato francese»[97]. Ove si dovesse ritenere sussistente il diritto della difesa di contraddire in merito alla correttezza del decrittaggio delle chat, il Giudice, nell'ottica di attuare la cooperazione cui, tra l'altro, si riferisce il trentesimo considerando della Direttiva, potrebbe, al fine di disporre eventuale perizia su detto aspetto, chiedere all'Autorità giudiziaria estera di fornire il relativo algoritmo; ciò ai sensi dell'art. 34, comma l, d.lgs. n. 108 del 2017, che, replicando la previsione dell'art. 8 della direttiva, contempla espressamente la possibilità che un ordine di indagine venga emesso, nello stesso o in altro procedimento, ad integrazione o completamento di uno precedente. Aderendo a questa impostazione l'impossibilità per le difese di conoscere i messaggi di testo in originale, le procedure di acquisizione da parte dell'Autorità francese e, infine, le modalità di decriptazione delle conversazioni oggetto di intercettazioni, potrebbe tradursi in irragionevole compromissione del suddetto principio[98]. Oltre a non poter esercitare il proprio diritto di difesa sulla scorta del segreto di Stato francese[99] con accettazione forzata dei dati trasmessi tramite O.I.E. e presunta scontata la ritualità delle procedure acquisitive poste in essere dall'A.G. francese (in virtù del principio del mutuo affidamento), si solleverebbe, di fatto, il Giudice nazionale dalle funzioni di valutazione e controllo sulla legittimità della prova, minandone l'indipendenza funzionale; quest'ultima, invece, attiene al momento di applicazione della legge e si traduce nel divieto da parte di altre autorità (anche quelle estere) di comprimere tale peculiare funzione giudiziale, impartendo ordini o suggerimenti circa il modo di giudicare in concreto. Del resto, sempre richiamando l'esperienza giudiziale maturata per altra tecnologia di comunicazioni criptate (Blackberry), la Cassazione ha offerto la possibilità alle difese di ottenere, non solo, la versione originale e criptata dei messaggi; inoltre, anche le chiavi di sicurezza necessarie per la lettura in chiaro degli stessi[100]. Cosi tale ricostruzione non trova rassicurante il richiamo alla impossibilità di alterazioni o manipolazioni dei testi captati per errato utilizzo dell'algoritmo per la decriptazione; se la scienza informatica assicura la fedele riproduzione, trattandosi di operazione *on*/*off*, salvo l'allegazione di specifici elementi di segno contrario, restano ignote (perché coperte dal segreto di Stato francese) le modalità di conservazione dei dati, le procedure e soggetti che hanno effettuato la masterizzazione su CD-ROM dei dati trasmessi con O.I.E. ai diversi Uffici di Procura italiani, nonché quelli che sono entrati in contatto con tali dispositivi magnetici; ragioni che quantomeno in via astratta – indurrebbero a ritenere ragionevole il pericolo che detti dati possano aver subito una manipolazione o alterazione. Incertezza che non riceve consolazione dalle ragioni sottese ai principi di mutua fiducia e del reciproco riconoscimento atteso

[97] Cass. Sez. VI, 26/10/2023, n. 46833, Bruzzaniti, cit.

[98] M. RAMPIONI, op. cit. pp. 26 e ss.

[99] Conseil constitutionnel, 8 aprile 2022 n. 2022-987, M. Said Z., in *www.cortecostituzionale.it* (servizio studi Area di diritto comparato) «La questione di costituzionalità sollevata dalla Corte di cassazione atteneva a mezzi di ricerca della prova nel procedimento penale che coinvolgessero strumenti di captazione di dati informatici. In particolare, si contestava la possibilità, per il procuratore della Repubblica, in sede di inchiesta, e per il giudice istruttore, durante l'istruttoria formalizzata, di ricorrere a strumenti di captazione coperti dal segreto di Stato. L'utilizzo di tali strumenti, possibile nell'ambito di procedimenti aventi a oggetto reati di criminalità organizzata, si riteneva che ledesse le garanzie processuali, in ragione del segreto opponibile e della conseguente limitazione del contraddittorio sul punto delle tecniche di captazione utilizzata. Il Conseil constitutionnel ha sottolineato, in primo luogo, come le previsioni contestate si fondino sulla necessità di contemperare, da un lato, le esigenze di ricerca degli autori dei reati e della repressione di questi e, dall'altro, quelle di protezione della sicurezza dello Stato. In secondo luogo, si impone alle autorità procedenti di dare adeguatamente conto delle ragioni per le quali si proceda attraverso strumenti coperti da segreto. In terzo luogo, si chiarisce che nel fascicolo istruttorio tutte le informazioni ottenute vengono riversate, così come le motivazioni addotte per il ricorso allo strumento protetto, con il che l'unico elemento sottratto al contraddittorio è la tecnica di captazione coperta dal segreto di Stato. Infine, qualora ne ravvisi le condizioni, la giurisdizione può richiedere la rimozione del segreto di Stato. In ragione di queste considerazioni, il Conseil ha ritenuto che la conciliazione tra interessi confliggenti possa dirsi adeguata e che quindi le disposizioni censurate non sia lesive della Costituzione».

[100] Cass., Sez. IV, 15 ottobre 2019, n. 49896, in *www.dejure.it*.

che il momento di valutazione dell'utilizzabilità della prova estera non può che avvenire secondo le regole dettate dall'ordinamento in cui quella prova è chiamata ad esprimere il suo contenuto conoscitivo[101]; motivo per cui in presenza di un dubbio che la prova straniera possa porsi in contrasto con i principi dell'ordinamento giuridico, il giudice italiano dovrebbe vanificarne il risultato conoscitivo.

In senso contrario, un diverso orientamento di legittimità ha ritenuto che «, in tema di intercettazione di comunicazioni telematiche, l'uso dell'algoritmo per la decriptazione della messaggistica con sistema Blackberry **esclude la possibilità di alterazioni o manipolazioni** dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici e concreti elementi di segno contrario» (tra le altre, Sez. 3, n. 30395 del 21/04/2022, Chiancano, Rv. 283454- 01) e che «il difensore delle parti ha diritto di accesso al dato trasmesso in via digitale costituito dalle sequenze alfanumeriche o simboliche rappresentative della comunicazione oggetto di captazione (c.d. stringhe) e dal risultato della decodificazione intellegibile di tali sequenze, in quanto elementi integranti "informazione" o "registrazione" delle conversazioni o comunicazioni ai sensi dell'art. 268, comma 7, cod. proc. pen. (Sez. 3, n. 38009 del 10/05/2019, Assisi, Rv. 278166- 02). In tale ultima pronuncia si è in particolare precisato (pag. 44) che la indisponibilità del programma di decrittazione dei "files" originari non è lesivo del diritto di difesa: «Innanzitutto, infatti, tale questione non riguarda l'utilizzabilità del dato, bensì l'affidabilità dello stesso (cfr., per questo rilievo, Sez. 6, n. 1342 del 04/11/2015, dep. 2016, Brandimarte, Rv. 267184-01)[102]». Nello stesso senso, con riferimento alle chat intercorse su piattaforma "SkyEcc", si è espressa di recente Cass., Sez. 6, n. 48838 del 2023, cit., secondo cui «Il diritto di difesa **non può, inoltre, essere ritenuto leso per effetto della mancata conoscenza** (e, dunque, dell'indisponibilità per la difesa) **dell'algoritmo** utilizzato per la decriptazione della messaggistica acquisita, qualificato come «segreto di sicurezza nazionale» dall'autorità francese, come risulta nella sentenza Conseil constitutionnel francese, con la decisione n. 2022-987 QPC dell'8 aprile 2022. Il difensore dell'indagato, nell'ordinamento italiano, può, infatti, 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». Nella medesima prospettiva può altresì essere richiamata, da ultimo, Cass. Sez. VI, n. 46390 del 26/10/2023, Rosaci, Rv. 285494 - 01, che in un *obiter dictum* ha confermato tale indirizzo ermeneutico, sostenendo che «In tema di mezzi di prova digitale, il sistema di diritto interno non garantisce alla difesa l'accesso agli algoritmi per la decodifica dei dati criptati, ma si limita a dettare garanzie procedurali a protezione della cd. "catena di custodia" nell'ottica dell'integrità probatoria, quali la necessità di un atto autorizzativo da parte di attori giudiziari qualificati, l'individuazione dei soggetti che possono acquisire e ritenere i dati e la disciplina della conservazione e consultazione degli stessi (Fattispecie relativa a dedotta inutilizzabilità, per mancata astensione del metodo di

[101] F. R. DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, op. cit., p. 144. Più in generale, in tema di ordine di indagine europeo il livello di tutela delle garanzie difensive non appare soddisfacente, risultando le stesse limitate sotto diversi profili: innanzitutto, dal debole coinvolgimento della difesa derivante dalla mancata piena conoscenza degli elementi posti alla base dell'emissione dell'ordine che rimangono circoscritti ad un dialogo riservato tra le autorità giudiziarie di emissione e di esecuzione, senza margini di intervento dell'indagato; poi, dall'insussistenza di un efficace sistema di eurodifesa che consenta un tempestivo contatto e coordinamento tra difensori operanti in diversi ordinamenti, con il conseguente rischio per il difensore straniero di veder limitato il proprio diritto di assistere al compimento delle operazioni investigativo-probatorie o di accedere prontamente agli atti del processo, indebolendo così la dialettica accusa-difesa.

[102] D'altra parte, poi, per quanto riguarda l'attendibilità della decodificazione, non solo, significativamente, l'operazione di decriptazione per l'autorità giudiziaria è effettuata dalla stessa azienda che garantisce l'ordinario e regolare svolgimento delle comunicazioni, e, quindi, la criptazione e decriptazione delle stesse, tra gli utenti dei dispositivi oggetto di intercettazione. Va infatti rilevato che «in assenza dell'algoritmo necessario alla decriptazione, risulta - secondo la scienza informatica - impossibile avere a disposizione un testo intellegibile in lingua italiana difforme dal reale, potendosi, al più avere, se del caso, una sequenza alfanumerica o simbolica ("stringa") priva di alcun senso», sicché, salvo l'allegazione di specifici e concreti elementi di segno contrario, deve escludersi l'avvenuta «manipolazione» delle captazioni (Cass. Sez. VI, n. 14395 del 27/11/2019, Testa, Rv. 275534-01).

decifrazione, delle "chat" criptate intercorse sulla piattaforma "Sky-Ecc" consegnate, tramite ordine europeo di indagine, dall'autorità giudiziaria francese a quella italiana con l'apposizione del segreto di Stato)». In detta pronuncia si è altresì rilevato che la conclusione cui è pervenuta, in senso contrario, la sentenza "Lori" non sarebbe pertinente atteso che essa è «relativa ad indagini acquisite tramite Europol, e non già tramite l'autorità giudiziaria e per mezzo di o.e.i., come invece nel caso in esame»: circostanza, questa, che tuttavia sembra contraddetta da quanto riportato a pag. 5 della stessa sentenza "Lori", ove si precisa che «le chat sono state formalmente acquisite al fascicolo tramite ordine europeo di indagine».

5. Il quadro giurisprudenziale delle Corti europee e le prospettive future.

Il diffondersi nei diversi paesi di indagini originate dai messaggi decriptati ha ingenerato molteplici contestazioni di vizi e di opacità nell'assunzione delle prove, di violazione delle norme sulla cooperazione giudiziaria transfrontaliera, nonché del diritto ad un processo equo e della *privacy*.

Può essere utile considerare l'evoluzione registratasi presso la giurisprudenza francese, tedesca e britannica. In questi Paesi i difensori hanno sostenuto che i messaggi ottenuti attraverso l'infiltrazione di EncroChat sarebbero inammissibili quali prove giudiziarie. In due lettere aperte, centinaia di avvocati, molti dei quali coinvolti nella difesa degli utenti, hanno ritenuto ingiusti i processi nei quali i pubblici ministeri si rifiutavano di rivelare informazioni sulle operazioni di *hacking*.

In **Francia**, gli avvocati hanno contestato, ad esempio, (*i*) l'assenza di limiti temporali per le misure di intercettazione nelle ordinanze del tribunale, (*ii*) l'autorizzazione di misure di ampia portata attraverso ordinanze del tribunale ritenute prive di basi giuridiche, (*iii*) l'intercettazione "massiccia e indiscriminata" e (*iv*) il rifiuto della Gendarmeria di divulgare eventuali dettagli tecnici dell'operazione di intercettazione. Al contrario, Eurojust ha ritenuto che l'indagine francese sia stata condotta in conformità con le norme giuridiche applicabili. La Gendarmeria francese ha dichiarato di aver ottenuto un parere favorevole sulla valutazione dell'impatto dei dati da parte dell'Autorità francese per la protezione dei dati personali (CNIL). Inoltre, la procedura è stata stimata compatibile con la Costituzione. In data 8 aprile 2022 il *Conseil consitutionelle* ha statuito che le disposizioni del codice penale che consentono agli investigatori di segretare le informazioni tecniche nell'interesse della difesa nazionale non violano i diritti degli imputati a un ricorso giurisdizionale effettivo e alla *privacy*, la libertà di espressione, o qualsiasi altro diritto garantito dalla Costituzione[103]. Per inciso, la decisione richiama l'attenzione sui requisiti legali e sulla necessaria divulgare determinate informazioni per giustificare l'esclusione del contraddittorio su alcune informazioni tecniche. La *Cour de Cassation* con sentenza n. 00592 del 12 aprile 2022 respinge il ricorso, avverso la sentenza emessa dalla Corte di Appello di Parigi, proposto dai titolari di Sky Global (società fornitrice degli apparati telefonici criptati), confermando l'applicabilità della legge francese e la competenza dei tribunali francesi a giudicare gli imputati, in quanto: *i*) i due *server* appartenenti alla società in questione risultavano installati sul suolo nazionale (francese); *ii*) il transito di tutte le conversazioni delle varie reti criminali avveniva sul suolo transalpino; *iii*) i rivenditori degli apparecchi telefonici Sky-Ecc erano stati identificati in Francia; *iv*) infine, gli utenti erano impegnati nel traffico di droga e nella trasformazione di denaro contante in bitcoin su suolo francese. Nondimeno, l'11 ottobre 2022 sempre la *Cour de cassation* ha ritenuto che la Corte d'appello non avesse adeguatamente tenuto conto dell'assenza di un certificato convalidando i risultati delle operazioni, annullando parzialmente l'impugnata decisione della Corte di Nancy, rimettendo la causa alla Corte d'Appello di Metz per una nuova sentenza; per ragioni simili, due settimane dopo ha parzialmente annullato un'altra decisione

[103] In particolare, è ritenuto la conformità costituzionale delle norme con riferimento all'art. 230, comma 1, c.p.p. francese, che consentono al Pubblico ministero, nel corso dell'indagine, e al giudice istruttore, in fase d'istruzione, di avvalersi dei mezzi dello Stato sottoposto al segreto di difesa nazionale per svolgere le operazioni tecniche necessarie all'acquisizione e all'estrapolazione dei dati, con l'effetto di schermare le informazioni relative a tali mezzi dal contraddittorio.

della Corte d'Appello di Nancy, deferendo il caso alla Corte d'Appello di Parigi. I casi francesi potrebbero influenzare procedimenti giudiziari e sfide legali in tutta Europa, che si basano sulle informazioni fornite dalle autorità francesi e sull'esistenza di un cd. "buco nero" probatorio.

Finora, presso il **Regno Unito**, il tribunale amministrativo, parte dell'Alta Corte inglese, ha respinto la richiesta di autorizzazione al controllo giurisdizionale dell'OEI su cui si basava l'azione penale e la Corte d'Appello ha stabilito che le comunicazioni raccolte erano ammissibili come prova, mentre la contestazione delle prove davanti alla Corte Suprema non è stata riconosciuta.

Al contrario, i pubblici ministeri tedeschi hanno subito una battuta d'arresto quando il **tribunale regionale di Berlino** ha ritenuto che i messaggi EncroChat costituivano prove inammissibili nel luglio 2021, in quanto ottenute in violazione della direttiva europea sull'ordine di indagine, in assenza di un livello sufficiente di sospetto a fondamento delle misure di sorveglianza. Ha pertanto riconosciuto la violazione del diritto costituzionale fondamentale alla riservatezza e all'integrità dei sistemi informatici, nonché al segreto delle telecomunicazioni. Il Tribunale regionale superiore di Berlino ha annullato la decisione nell'agosto 2021, in linea con numerose altre sentenze dei tribunali regionali superiori di tutta la Germania (ad esempio Karlsruhe, Brandeburgo, Düsseldorf, Rostock, Schleswig). Solo il tribunale regionale di Francoforte ha condiviso la posizione del Tribunale regionale di Berlino. In una recente decisione, la Corte Suprema Federale ha stabilito che i dati di EncroChat possono essere utilizzati per indagare su reati gravi.

Il Tribunale regionale di Berlino ha recentemente richiesto una pronuncia pregiudiziale alla Corte di giustizia dell'Unione europea su quattordici punti critici con domande riguardanti un altro caso EncroChat. Come detto, il funzionamento del trojan utilizzato dalla polizia francese non è attualmente conosciuto, né conoscibile, in quanto protetto dal segreto militare francese. Allo stesso modo, le autorità tedesche non hanno mai divulgato neppure le informazioni non segrete che hanno appreso in merito dai colleghi francesi. Le iniziali modalità di comunicazione dei dati da parte dei francesi, inoltre, non erano note nei primi procedimenti in Germania. Pertanto, i Tribunali tedeschi hanno basato le loro decisioni, tanto cautelari, quanto di merito, sul presupposto che le risultanze investigative alla base dei procedimenti fossero state inviate "spontaneamente" alle autorità tedesche e che non vi fosse stato un ruolo attivo di raccolta di queste ultime da parte degli investigatori tedeschi. Al contrario, è poi emersa la possibilità che nella fase iniziale vi sia stato **uno scambio informativo informale**, nell'ambito del quale le autorità tedesche abbiano attivato il monitoraggio degli utenti EncroChat in Germania a fini penali, servendosi dell'attività già in corso in Francia. Verrebbe in rilievo, perciò, un'attività investigativa che si sarebbe dovuta basare fin dall'inizio su un OIE, in modo da poterne successivamente vagliare la legittimità ai sensi del diritto tedesco e garantire quindi i diritti fondamentali degli indagati (tramite la verifica della necessità e proporzionalità dell'ordine nonché della legittimità dell'attività d'indagine rispetto al diritto interno). Già in passato, infatti, la stessa CGUE (Corte di Giustizia UE, sentenza del 2 marzo 2021, La Quadrature du Net e altri – C-511/18) ha sottolineato come la trasmissione ad un'autorità di dati relativi al traffico o all'ubicazione sia di per sé una grave compressione dei diritti fondamentali di cui agli artt. 7 e 8 della Carta. A parere del Giudice tedesco, sulla base della giurisprudenza europea ciò è ancora più necessario laddove le prove in questione siano il frutto di un ambito tecnico rispetto al quale né il giudice né le parti hanno competenza[104]. L'utilizzabilità dei dati di EncroChat sarebbe pertanto messa in discussione dall'impossibilità, attuale, di valutarne le modalità tecniche di intercettazione, dirottamento, archiviazione ed estrazione. L'esercizio del diritto di difesa, infatti, verrebbe compromesso in assenza della possibilità di verificare la correttezza, completezza e coerenza dei dati utilizzati in giudizio. Peraltro, in molti casi, i dati delle chat EncroChat costituiscono l'unica prova in relazione al fatto contestato. Per integrare il reato di traffico di stupefacenti sarebbe già sufficiente la prova di trattative sulla vendita delle sostanze e per la difesa è fondamentale poter valutare sia i singoli messaggi che il

[104] Cfr. Corte di giustizia UE, sentenze del 2 marzo 2021 H.K./Prokuratuur – C-746/18, La Quadrature du Net e altri – C-511/18, e del 10 aprile 2003 Steffensen – C-276/01; Corte EDU, decisione del 18 marzo 1997, Mantovanelli/Francia.

rapporto temporale e contenutistico esistente tra messaggi inviati e ricevuti. Infatti, errori di natura tecnica o incompletezze potrebbero distorcere il significato delle chat senza che poi sia possibile avvedersene avendo a disposizione solo gli esiti dell'attività investigativa. Secondo i criteri elaborati dalla Corte di Giustizia nella sentenza Steffensen[105], basterebbe il solo fatto che i dati utilizzati non possano essere verificati dalle difese tramite un consulente tecnico per dedurne l'inutilizzabilità come prove. Ad aggravare tale compressione si è aggiunto il rifiuto delle agenzie europee e delle autorità tedesche di rendere accessibili documenti non sottoposti al segreto militare francese e che sarebbero però stati rilevanti per la difesa. In particolare, è stato stigmatizzato il rifiuto di condividere i messaggi scambiati dalle autorità tedesche attraverso il sistema SIENA[106] e che avrebbero consentito almeno di verificare se durante la fase iniziale della cooperazione con gli investigatori francesi siano state comunicate anomalie tecniche nonché rispetto a quali dati. Inoltre, la Corte tedesca ha sottolineato come la costante giurisprudenza europea abbia stabilito che il contrasto a reati gravi non può in alcun modo giustificare una conservazione indiscriminata e generalizzata di dati. Infatti, vi sono state pronunce che hanno consentito l'accesso a fini penali a dati precisi sul traffico e sull'ubicazione, ma che al tempo stesso ne hanno vincolato la legittimità al rispetto del principio di proporzionalità, nonché alla presenza costante di un controllo da parte di un giudice o di un'autorità amministrativa indipendente. In questo caso (e in altri ad esso affini) difetterebbero entrambi i requisiti. La raccolta dei dati è stata effettuata su un campione di utenti enorme e indiscriminato (32.477 utenti su 64.134), senza che si potesse ritenere a priori una appartenenza di tutti i clienti di EncroChat ad un'unica rete criminale; né sono state indagate eventuali necessità di *privacy* molto rafforzata dovuta all'esercizio di attività lecite. Al contrario, è stata elaborata l'equazione per cui a determinati costi e funzionalità debba corrispondere necessariamente un servizio per attività illecite. **Inoltre, l'attività di impulso delle indagini in Germania non sarebbe derivata da attività sotto il controllo dell'autorità giudiziaria, ma sarebbe il frutto della cooperazione tra polizie coordinata dall'Europol**. Anche in seguito, quando è intervenuta la magistratura tedesca, sono stati acquisiti solo gli esiti di attività tecnica eseguita dal Joint Investigation Team su EncroChat ed in particolare dalla Gendarmerie. Si sarebbe così impedito sia un controllo *ex ante* da parte di un'autorità indipendente, sia un controllo *ex post* sotto forma dell'esercizio del diritto di difesa attraverso la prova nel contraddittorio tra le parti.

Conclusivamente il quadro che precede evidenzia l'ampia problematicità che sono chiamate a risolvere le Alte Corti nazionali e sovranazionali, in un quadro complesso e mutevole. Appare inevitabile, a chi scrive, ritenere che, in prospettiva futura, lo sviluppo e le potenzialità delle migliori tecnologie investigative vada conservato entro il perimetro del rispetto rigoroso delle garanzie fondamentali individuali e del giusto processo.

Tra queste ultime, difficilmente, potrà essere esclusa quella della possibilità di attivare un **controllo *ex post* sulla legittimità** del mezzo di ricerca utilizzato, sulla sua **proporzionalità** e sulla **attendibilità piena** del dato probatorio acquisito. La fiducia della correttezza, alla lunga, si costruisce sulla trasparenza della conoscenza e non sulla sicurezza del segreto.

[105] Cfr. Corte di giustizia UE, sentenza del 10 aprile 2003, Steffensen – C-276/01.

[106] *Secure Information Exchange Network Application* costituisce una piattaforma di comunicazione per le forze dell'ordine dell'Unione Europea.