PALMA PUJIA

L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali

L'implementazione spasmodica dei nuovi modelli digitali e la ventata di euforia che anima l'arrivo delle nuove tecnologie se, da un lato, offre molteplici opportunità di sviluppo specie in ambito investigativo, dall'altro genera varie problematiche legate all'agevolazione di alcune tipologie di reati. In tale prospettiva, particolare rilievo hanno assunto gli strumenti di messaggistica criptata, da ultimo la piattaforma Sky-ECC, oggi terreno fertile per la commissione di numerose attività illecite. Una risposta giudiziaria efficace a tale tipo di minacce richiede un'implementazione strumentale investigativa idonea a fronteggiare e, se possibile, arrestare detti fenomeni criminali.

È importante, naturalmente, che l'attività d'indagine avvenga nel rispetto dei diritti fondamentali dell'individuo e che le prove raccolte siano valide e ammissibili, in linea con la disciplina processuale vigente. Il bilanciamento tra esigenze repressive e tutela delle libertà fondamentali appare necessario in una realtà in continuo divenire, nella quale la "staticità" dell'importanza dei valori e dei diritti fondamentali costituisce un'esigenza da preservare.

Muovendo dall'*excursus* giurisprudenziale, per certi versi oscillante, della suprema Corte in tema di acquisizione all'estero della messaggistica criptata Sky-ECC e archiviata su *server* straniero, il presente scritto si propone di approfondire una tematica tuttora controversa, per comprendere quale debba essere la normativa interna applicabile. Per arrivare, infine, al recente *dictum* delle Sezioni unite che si propone di porre un punto fermo sull'argomento.

The acquisition of encrypted messaging stored on a foreign server between conceptual classifications and jurisprudential divergences

The spasmodic implementation of new digital models and the wave of euphoria that animates the arrival of new technologies, on the one hand, offers multiple opportunities for development especially in the investigative field, on the other hand generates various problems related to the facilitation of certain types of crimes. In this perspective, encrypted messaging tools have assumed particular importance, most recently the Sky-ECC platform, today fertile ground for the commission of numerous illicit activities. An effective judicial response to this type of threat requires an instrumental investigative implementation suitable for dealing with and, if possible, stopping said criminal phenomena. It is important, of course, that the investigative activity takes place in compliance with the fundamental rights of the individual and that the evidence collected is valid and admissible, in line with the current procedural discipline. The balance between repressive needs and the protection of fundamental freedoms appears necessary in a constantly evolving reality, in which the "static" nature of the importance of values and fundamental rights constitutes a need to be preserved. Starting from the jurisprudential excursus, in some ways oscillating, of the Supreme Court about the acquisition abroad of Sky-ECC encrypted messaging and archived on a foreign server, this paper aims to delve into a still controversial topic, to understand

what the applicable internal legislation should be. Finally, to arrive at the recent dictum of the United Sections that aims to put a full stop on the subject.

SOMMARIO: Premessa 1. Comunicazioni criptate e processo penale. 2 La natura giuridica problematica dell'attività di acquisizione delle chat conservate su piattaforme criptate. 3 L'acquisizione all'estero della messaggistica archiviata su piattaforma SKY-ECC: orientamenti giurisprudenziali a confronto. 4. La presa di posizione delle Sezioni unite.

1. *Comunicazioni criptate e processo penale.* Il mondo del diritto è stato massivamente interessato negli ultimi anni dall'impatto prospettico, talvolta già realizzato, dell'evoluzione tecnologica in ambito informatico. L'irruenza del mondo digitale nel processo penale, se da un lato mette in evidenza la profonda distanza sussistente tra *techne* e *ratio*, suscitando una serie di interrogativi, dall'altro evidenzia l'importanza di comprendere e affrontare le implicazioni che il progresso della tecnologia comporta. Preconizzando il predominio potenziale, se non già effettuale, della *techne* sulla psiche il filosofo Umberto Galimberti ricorda che «abitiamo la tecnica irrimediabilmente e senza scelta. Questo è il nostro destino di occidentali avanzati, e coloro che, pur abitandolo, pensano ancora di rintracciare un'essenza dell'uomo al di là del condizionamento tecnico, come capita di sentire, sono semplicemente degli inconsapevoli»[1].

Il condizionamento tecnologico pone al giurista problemi di continuo aggiornamento e adeguamento delle categorie concettuali ai nuovi fenomeni. Gli strumenti tecnologici non sono buoni o cattivi in sé, giacché è il modo in cui vengono impiegati che ne condiziona, com'è evidente, gli effetti sui contesti nei quali incidono, sicché il progresso tecnologico è, al tempo stesso, matrice di straordinarie opportunità e fonte di rischi considerevoli.

Tutto ciò appare evidente in un ambito, come quello del processo penale, nel quale vengono in gioco e sono continuamente sollecitati e messi in discussione i diritti fondamentali della persona umana, costituzionalmente riconosciuti e garantiti.

Per un verso, le nuove tecnologie forniscono importanti risorse in ambito investigativo[2], garantendo strumenti d'accertamento di straordinaria efficacia; per altro verso, però, esse agevolano considerevolmente la stessa commissio-

[1] GALIMBERTI, *Psiche e Techne. L'uomo nell'era della tecnica*, Milano, 1999, 34.

[2] LORUSSO, *Digital evidence, cybercrime e giustizia penale 2.0.*, in *Proc. pen. giust.*, 2019, 4, 2.

ne di reati di particolare rilevanza, anche, e soprattutto, da parte delle grandi organizzazioni criminali che operano su scala internazionale.
Un recente esempio, emblematico di tecnologia le cui potenzialità pone problemi di non poco conto in ambito processuale, è rappresentato da uno strumento quale la piattaforma digitale SKY ECC, che consente lo scambio di comunicazioni attraverso i cc.dd. "criptofonini", vale a dire *smartphone* dotati di un particolare *software* (per lo più con sistema *Blackberry*) che consentono di garantire l'inviolabilità della comunicazione da parte di soggetti estranei alla stessa[3]. In particolare, il sistema operativo di tali *smartphone* è caratterizzato da stringenti requisiti di sicurezza, consistenti nella cifratura dei dati trasmessi e di quelli memorizzati, nella possibilità di segnalare la presenza di sistemi di spionaggio o di individuazione volti ad aggredire il sistema in questione e nella possibilità per il fruitore del sistema operativo di eliminare, quasi tempestivamente e da remoto, l'intera memoria del telefono attraverso l'inserimento del c.d. "*panic code*".
Tali piattaforme non si basano sulla tecnologia c.d. *pin to pin*, la quale consente di scambiare comunicazioni scritte attraverso un programma che sfrutta il sistema telematico creato dalla casa produttrice dei medesimi dispositivi[4], bensì su un sistema maggiormente protetto denominato "*end to end*.", il quale si basa sulla cifratura delle conversazioni attraverso l'utilizzo di chiavi depositate esclusivamente nei dispositivi utilizzati dai comunicanti.
Ne deriva che neanche il gestore del servizio sarà in grado di apprendere le chiavi utilizzate e, di conseguenza, il contenuto della comunicazione. La crittografia *end to end*. risulta, pertanto, ben più sicura, in quanto permette soltanto ai comunicanti di decriptare e, quindi, di decifrare i messaggi inviati e ricevuti. L'utilizzo della piattaforma SKY ECC, sfruttando la crittografia *end to end.*, risulta apparentemente impenetrabile e non assoggettabile ad alcuna forma di controllo. Ed è proprio tale caratteristica a far sì che la piattaforma in esame venga utilizzata dalle organizzazioni criminali per realizzare attività illecite, determinando la necessità per chi svolge attività investigative di impie-

[3] Sul tema cfr. diffusamente, da ultimo, MURRO, *Lo* smartphone c*ome fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Milano, 2024, *passim*, nonché CURTOTTI-RIZZI-NOCERINO-RUSSITTO-GILIBERTI-SCARPA, *Piattaforme criptate e prova penale,* in *Sist. pen.*, 2023, 6, 173 ss.
[4] Sul punto, cfr. TROGU, *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry*?,* in *Proc. pen. giust.,* 2016, 3, 3; TESTAGUZZA, Chat Blackberry*: il sistema "*pin to pin*". Nascita di un nuovo paradiso processuale*, in *questa Rivista,* 2016, 2, 6.

gare tecniche d'indagine idonee a superare le "barriere" difensive poste da tali strumenti[5].

È in tale contesto di fondo che si colloca l'attività interpretativa della Corte di cassazione caratterizzata, in assenza di un dato normativo lineare, da divergenze significative sul punto che si sono tradotte in un'evidente antinomia contenutistica. Anche se la recente risposta offerta dalle sentenze delle Sezioni Unite del 29 febbraio 2024 pone qualche punto fermo in ordine a profili estremamente controversi riguardanti l'acquisizione della messaggistica criptata e archiviata su server straniero, suggerendo una riflessione complessiva su un tema concettualmente complesso[6].

In precedenza, diverse pronunce dei giudici di legittimità hanno sostenuto la possibilità di acquisire le chat criptate ai sensi dell'art. 234 *bis* c.p.p. (il quale consente l'acquisizione di documenti e dati informatici conservati all'estero), sulla base della distinzione tra intercettazioni, implicanti la captazione, e attività di acquisizione e decifrazione di dati comunicativi[7].

Altre sentenze della Corte di cassazione, invece, hanno accolto un differente indirizzo interpretativo, affermando che l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY ECC non costituisce dato informatico, bensì vero e proprio flusso comunicativo; sicché l'attività di acquisizione, se riguardante comunicazioni avvenute nella fase "dinamica", dev'essere inquadrata nella disciplina delle intercettazioni telematiche *ex* artt. 266 e ss. c.p.p.; se riguardante, invece, comunicazioni avvenute nella fase "statica", dev'essere assoggettata alle disposizioni in materia di perquisizione e sequestro di cui all'art. 254 c.p.p.[8].

Occorre fin da ora evidenziare come, dietro gli aspetti squisitamente tecnici, si celino, in realtà, bilanciamenti di valori diversi, coinvolgenti, da un lato, le esigenze di efficienza dell'azione investigativa e, dall'altro, i diritti fondamenta-

[5] Il *novum* di tali tecniche d'indagine, si afferma in dottrina, non consiste nel rinnovare lo strumento con il quale esperire le investigazioni, ma nel considerare un nuovo spazio d'indagine: *«quello del server sul quale transitano tutti i flussi informativi degli utenti che utilizzano le piattaforme criptate»* (cfr. ancora CURTOTTI-RIZZI-NOCERINO-RUSSITTO-GILIBERTI-SCARPA, *Piattaforme criptate,* cit.).

[6] Più ampiamente, sul tema della circolazione di dati tra autorità giudiziarie dei paesi dell'Unione europea, si rimanda a TROISI, *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012, 12.

[7] Cfr. Cass., Sez. I, 18 gennaio 2024, n. 2312., in *Proc. pen. giust.,* 2024, 2.

[8] Sul punto, Cass., Sez. VI, 2 novembre 2023, n. 44154, in *Cass. pen.,* 2024, 1, 162 ss.

li costituzionalmente garantiti, in particolare quelli riconosciuti dall'art. 15 Cost.

2. *La natura giuridica problematica dell'attività di acquisizione delle* chat *conservate su piattaforme criptate.* La prima questione da affrontare in riferimento all'acquisizione delle *chat* su piattaforme criptate è quella della natura giuridica di tale attività. Si tratta, com'è evidente, di un profilo preliminare alla definizione di tutti gli altri aspetti rilevanti: il problema dell'utilizzazione, nell'ambito del processo penale, dei risultati investigativi ottenuti all'estero e quello delle garanzie procedimentali che dovrebbero accompagnare l'attività d'indagine condotta con i tipi di intervento in esame.
La giurisprudenza di legittimità[9] ha chiarito che occorre distinguere due diversi tipi di operazioni che gli organi inquirenti possono effettuare nello svolgimento dell'attività d'indagine[10]: una prima, avente a oggetto la captazione di un flusso comunicativo o di una registrazione di un messaggio cifrato nel momento in cui lo stesso è in transito dall'apparecchio del mittente a quello del destinatario; una seconda, consistente nella decriptazione del contenuto del messaggio volta a trasformare mere stringhe informatiche in dati comunicativi intellegibili.
La Cassazione, nel valutare la natura giuridica dell'acquisizione delle *chat* su piattaforma criptata, in un primo momento ha considerato l'operazione avente a oggetto la captazione di una comunicazione in tempo reale rientrante nel novero della disciplina delle intercettazioni *ex* art. 266 *bis* c.p.p.; mentre invece la seconda operazione, basandosi sulla decriptazione di un messaggio archiviato su *server* (straniero), è stata fatta rientrare nel novero della disciplina attinente alla prova documentale (art. 234 *bis* c.p.p.)[11].
In base a tale orientamento, l'attività di acquisizione e di decifrazione dei dati, quindi, non sarebbe assoggettabile alla disciplina delle intercettazioni[12], la qua-

[9] NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla* querelle *giurisprudenziale sull'acquisizione di messagistica criptata dall'estero*, in *sistemapenale.it*, 27 febbraio 2024.
[10] V., tra le altre, Cass., Sez. I, 15 febbraio 2023, n. 6364, in *www.sistemapenale.it,* 18 dicembre 2023; cfr. anche Cass., 1° luglio 2022, n. 34059, in *www.cortedicassazione.it.*
[11] Cass., Sez. III, 25 settembre 2019, n. 47557.
[12] Nella stessa direzione: cfr. Cass., Sez. IV, 5 aprile 2023, n. 16347, in *Proc. pen. giust.,* 2023, 6, 1318 ss.; Cass., Sez. I, 13 gennaio 2023 n. 19082; Cass., Sez. VI, 20 aprile 2021, n. 18907. Secondo questi arresti giurisprudenziali (in particolare il rinvio è a Cass., Sez. IV, 5 aprile 2023, n. 16347), la messagi-

le postula un'attività di captazione di comunicazioni in tempo reale. Inoltre, trattandosi di rappresentazioni comunicative incorporate su base materiale con un metodo digitale, ovvero di dati che hanno consentito di rendere intellegibile il contenuto di stringhe redatte secondo il sistema binario, risulta applicabile la disciplina della prova documentale. Trattandosi poi di dati non disponibili al pubblico, in questi casi vi sarebbe stato il consenso da parte del legittimo titolare all'acquisizione, richiesto dall'art. 234 *bis*[13]: soggetto 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, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*Internet service provider*»[14].

Dal punto di vista letterale, d'altro canto, la definizione di intercettazione adottata dalle Sezioni Unite nel 2002 fa leva sulla captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscono con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del carattere riservato della comunicazione[15]. A rigore, pertanto, si dovrebbe parlare di intercettazione solo con riferimento a una captazione contestuale della comunicazione. Ma quanto appena detto può considerarsi sufficiente al fine di valutare l'approvvigionamento di *chat*, salvate su *server*, alla stregua di meri documenti?

---

stica su *chat* di gruppo su sistema "Sky ECC", acquisita mediante OEI (Ordine di indagine europeo) da autorità giudiziaria straniera che ne ha eseguito la decriptazione, costituisce dato informativo documentale conservato all'estero, utilizzabile ai sensi dell'art. 234 *bis* c.p.p. e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266 *bis* c.p.p.

[13] L'art. 234 *bis* c.p.p., come introdotto dal d.l. 18 febbraio 2015, n. 7, convertito in L. 17 aprile 2015, n. 43, è stato introdotto nel quadro della lotta al terrorismo e ai c.d. *foreign fighters* (coloro che si fanno arruolare per compiere atti di terrorismo). Secondo il nuovo disposto, è sempre ammessa l'acquisizione di documenti e dati informatici conservati all'estero, anche di quelli non disponibili al pubblico, purché in quest'ultimo caso vi sia il consenso del legittimo titolare.

[14] Così Cass., Sez. I, 15 febbraio 2023, n. 6364, cit.; Cass., Sez. I, 1° luglio 2022, n. 34059, cit.;

[15] Cass., Sez. un., 24 settembre 2003, n. 36747, in *Arch. nuova proc. pen.*, 2003, 6, 540.

Una risposta positiva a tale domanda finirebbe per offrire risposte fin troppo formalistiche, eccessivamente astratte, che non terrebbero conto dei caratteri peculiari della messaggistica digitale.
Tuttavia, è possibile un'interpretazione evolutiva dell'art. 15 Cost. che, come si vedrà, è stata ripresa in una successiva sentenza[16], secondo cui nel concetto di corrispondenza rientrano anche la posta elettronica e i messaggi inviati tramite sistemi di messaggistica istantanea; la tutela apprestata dall'art. 15 Cost., sostiene la Consulta, prescinde dalle caratteristiche del mezzo tecnico utilizzato ai fini della trasmissione del pensiero. Non v'è dubbio, del resto, che nella realtà odierna la posta elettronica rappresenti la versione informatica della corrispondenza cartacea. D'altronde, tale indirizzo trova conferma anche nel diritto penale, ove l'equiparazione tra posta elettronica e posta cartacea è normativamente prevista dall'art. 616 c.p.[17].
È anche vero, peraltro, che il trasferimento ai prodotti del mondo immateriale di concetti originariamente concepiti per il mondo materiale deve essere eseguito con particolare cautela, al fine di evitare pericolose semplificazioni.
In particolare, come hanno mostrato alcuni recenti studi sul linguaggio impiegato nella giurisprudenza delle Corti supreme relativa alla tutela dei diritti fondamentali nella dimensione digitale, l'adozione di un punto di vista "interno"[18] alla dimensione tecnologica, esprimentesi nell'accettazione di certe costruzioni metaforiche utilizzate per descrivere il mondo digitale, condiziona sensibilmente i risultati interpretativi di giudici e Corti. Così come, di contro, il rifiuto di tale prospettiva e la scelta di un punto di vista "esterno" alla medesima dimensione orientano verso esiti opposti[19]. In altri termini, prendendo sul serio il modo in cui le nuove tecnologie soddisfano le diverse, attuali esigenze umane si è maggiormente propensi ad accogliere interpretazioni estensive ed evolutive delle previsioni normative delle garanzie dei diritti coinvolti dall'uso delle medesime tecnologie.
Di conseguenza, valutare la funzionalità della messaggistica istantanea e della posta elettronica – comprendendone a fondo il meccanismo d'azione – im-

[16] Corte cost., 27 luglio 2023, n. 170.
[17] Norma che così recita: «agli effetti delle disposizioni di questa sezione per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza».
[18] HART, *Il concetto di diritto*, a cura di Cattaneo, Torino, 2002, *passim*.
[19] Cfr. MORELLI-POLLICINO, *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Riv. AIC*, 2018, 1, 1 ss.

plica una considerazione di non poco conto: la comunicazione tradizionale che si instaura tramite lettera (scambio epistolare) non può essere assimilata *in toto* alla comunicazione che si instaura tramite piattaforme di messaggistica istantanea o posta elettronica. Quest'ultimo tipo di contatto, in virtù delle potenzialità che caratterizzano i mezzi comunicativi richiamati, introduce una dimensione inedita di comunicazione, più difficilmente gestibile rispetto a quella classica. Si pensi, per esempio, all'immediatezza e alla rapidità che caratterizzano lo strumento della messagistica istantanea, in contrapposizione alla tradizionale esperienza di scrittura.
Si può facilmente intuire, quindi, come la strutturazione dell'immaginario consequenziale a questo modo di comunicare plasmi interamente le nostre vite: parlare ed essere immersi in un mondo virtuale fa sì che la soggettività umana prenda forma in una complessità più ampia. Nelle *chat* sorge la rappresentazione di sé e dell'altro; potremmo parlare di una sorta di stanza "dei riflessi". Di conseguenza il concetto di *digital communication* travalica quello di corrispondenza tradizionale, esigendo probabilmente una tutela rafforzata.
Si tornerà più avanti su tali aspetti; per il momento, è sufficiente rilevare che l'interpretazione fornita dalla giurisprudenza di legittimità prima richiamata, rendendo meno macchinoso il procedimento di acquisizione delle *chat* archiviate su *server* straniero, si muove seguendo una logica efficientista, con l'effetto di indebolire sensibilmente le garanzie poste a presidio della persona sottoposta alle indagini.

3. *L'acquisizione all'estero della messaggistica archiviata su piattaforma SKY-ECC: orientamenti giurisprudenziali a confronto.* Una diversa sensibilità verso le esigenze di protezione della libertà di comunicazione nelle più avanzate modalità consentite dalla tecnologia si rinviene, invece, nella sentenza n. 44154/2023 della Corte di cassazione[20], che ha decisamente rigettato l'indirizzo prima richiamato affermando che «l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY ECC non costituisce dato informatico utilizzabile ai sensi dell'art. 234 *bis* c.p.p., bensì vero e proprio flusso comunicativo; sicché, in tale ipotesi, l'attività di acquisizione, se riguardante comunicazioni avvenute nella fase 'dinamica' dev'essere inquadrata nella disciplina delle intercettazioni telematiche ai sensi degli artt. 266 e ss.

[20] Sul tema NOCERINO, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni unite*, in *www.penaledp.it.*, 29 novembre 2023.

c.p.p., se riguardante, invece, comunicazioni avvenute nella fase 'statica' dev'essere assoggettata alle disposizioni in materia di perquisizione e sequestro ai sensi dell'art. 254 c.p.p»[21].

Si è così esclusa l'applicabilità dell'art. 234 *bis* c.p.p., con un netto distacco dall'orientamento[22] secondo il quale la messaggistica su *chat* di gruppo su sistema SKY ECC, acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne ha eseguito la decriptazione, costituisce dato informativo documentale. Si è ritenuto, così, che tale disciplina possa trovare applicazione solo nell'ipotesi di acquisizione di documenti e/o dati informatici "dematerializzati", i quali preesistevano rispetto all'inizio dell'attività d'indagine o che, comunque, si erano formati al di fuori di quella determinata attività investigativa.

Nel caso *de quo*, l'attività di acquisizione esperita dagli organi competenti è consistita, in effetti, solo in parte nell'acquisizione di documentazione preesistente, avendo avuto invece a oggetto, in larga parte, documentazione di attività di indagine. I dati erroneamente qualificati come "documenti informatici" sono stati oggetto di attività di decriptazione da parte dell'autorità giudiziaria straniera che, solo in un secondo momento, li ha trasmessi all'autorità giudiziaria italiana. Tale attività di decriptazione è stata eseguita dalle autorità francesi attraverso l'effettuazione di operazioni costituenti in parte una vera e propria intercettazione. Il che rende evidente l'incompatibilità applicativa dell'art. 234 *bis* c.p.p.

E invero, se da un lato risulta abbastanza chiara la non applicazione dell'art. 234 *bis* c.p.p. con riferimento all'acquisizione di dati e informazioni oggetto di comunicazione o corrispondenza scambiate in tempo reale tra due o più soggetti indagati in Italia[23], poiché, in questi casi, l'acquisizione dei dati costituirebbe un'intercettazione telematica avente a oggetto dati "dinamici", nel caso prospettato il nodo problematico da sciogliere concerne l'acquisizione all'estero di contenuti archiviati in un *server*, quindi riferibili a comunicazioni già avvenute. Ed ecco che proprio in relazione a tale tipo di acquisizione, nel giustificare l'applicazione dell'art. 254 *bis* c.p.p., riguardante le ipotesi di se-

[21] Così, Cass., Sez. VI, 2 novembre 2023, n. 44154, cit.; Cass., Sez. VI, 26 ottobre 2023, n. 44155.

[22] Appartenenti al filone giurisprudenziale opposto: Cass., Sez. IV, 5 aprile 2023, n. 16347, in *Proc. pen. giust.,* 2023, 6, 1318 ss.; Cass. Sez. I, 15 febbraio 2023, n. 6364, cit.

[23] ATERNO, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella* privacy, in *questa Rivista,* 2016, 1, 166.

questro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni, la Corte si richiama alla vigente normativa interna per l'acquisizione presso il *server* dei dati esterni alle comunicazioni, la quale, alla luce di alcune pronunce della Corte di giustizia dell'unione europea, è stata oggetto di profondi mutamenti, prevedendo che l'attività di acquisizione di tali dati sia preceduta dall'autorizzazione da parte dell'autorità giudiziaria. Tale attività, seppur risulti meno invasiva poiché avente a oggetto l'apprensione di dati esterni alle comunicazioni, deve necessariamente essere sottoposta al vaglio dell'autorità procedente che può o meno autorizzarla.
In particolare i giudici di legittimità, richiamando la sentenza del 2 marzo 2021 della Grande camera e sottolineando il grande impatto che quest'ultima ha avuto sul nostro ordinamento (decreto-legge 30 settembre 2021, n. 132)[24] – poiché ha permesso la "giurisdizionalizzazione"[25] della procedura di acquisizione dei dati esterni di traffico telefonico e telematico – evidenziano come l'accesso a tali dati debba essere circoscritto a procedure aventi per scopo la lotta contro forme gravi di criminalità e che non possa essere il pubblico ministero ad autorizzare l'accesso medesimo, distaccandosi dall'orientamento giurisprudenziale secondo cui nella nozione di intercettazione non dovrebbero rientrare le acquisizioni a fini probatori di notizie riguardanti il fatto storico dell'avvenuta comunicazione.
Ponendo un parallelismo tra l'attività di acquisizione di documenti conservati su *server* straniero avente oggetto comunicazioni già avvenute e l'attività di acquisizione di dati esterni alle comunicazioni, la Corte sostiene che sarebbe del tutto improponibile ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento da parte del giudice, mentre per il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero, trattandosi pur sempre di un flusso comunicativo che rientra a pieno titolo nel concetto di corrispondenza *ex* art. 15 Cost.

[24] Il decreto-legge n. 132 del 2021 costituisce un intervento normativo d'urgenza mediante il quale sono state inserite nuove disposizioni nell'art. 132 del Codice della *privacy*. Con il testo normativo in parola il legislatore, rompendo gli indugi dovuti alle aporie giurisprudenziali creatisi in seguito alla sentenza della Grande camera della Corte di giustizia del 2 marzo 2021, ha introdotto espressamente la necessità dell'intervento del giudice per l'acquisizione dei tabulati telefonici.
[25] Così, Cass., Sez. VI, 2 novembre 2023, n. 44154, cit.

La Cassazione, richiamando l'*iter* logico seguito dalla Consulta nel caso *Open*, riprende la distinzione tra i concetti di comunicazione "statica" e "dinamica", ribadendo la differenza tra l'attività di intercettazione, che concerne la captazione occulta da parte di un terzo di comunicazioni nella loro fase dinamica, e l'attività di sequestro, che attiene all'acquisizione del supporto recante memoria di comunicazioni già avvenute, cioè nella loro fase statica. L'attività acquisitiva in esame rientrerebbe nella seconda ipotesi, perché il concetto di corrispondenza risulta comprensivo della «corrispondenza elettronica, anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza trasformandosi in mero documento storico»[26] .

I confini dell'attuale portata applicativa dell'art. 15 Cost. risultano così estesi, in virtù dell'interpretazione evolutiva che ne ha offerto la Corte costituzionale, garantendo una lettura del testo particolarmente sensibile all'evoluzione dell'odierno contesto tecnologico e consentendo di comprendere nell'alveo della norma costituzionale ogni strumento che la rivoluzione «tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici in relazione ai quali le limitazioni della libertà costituzionale sono consentite solamente nel rispetto della riserva assoluta di legge e di giurisdizione»[27].

Anche la Corte di giustizia dell'unione europea, del resto, ha più volte sottolineato che l'acquisizione dei dati di traffico telefonico o telematico debba avvenire con modalità che garantiscano un adeguato vaglio giurisdizionale[28].

A seguire una direzione diametralmente opposta è invece la pronuncia della Corte di cassazione n. 2312 del 18 gennaio 2024[29], attestata sull'orientamento maggioritario secondo cui le conversazioni archiviate su server e acquisite all'estero su piattaforma SKY ECC hanno natura di documenti e non di intercettazioni. Muovendo dalla distinzione tra captazione e decriptazione, la Corte evidenzia come quest'ultima, consistendo nella trasformazione di stringhe informatiche in contenuti comprensibili tramite l'algoritmo fornito dalla società titolare del sistema operativo utilizzato, sia cosa ben diversa dalla cap-

[26] Corte cost., 27 luglio 2023, n. 170, cit.

[27] Così, Cass., Sez. VI, 2 novembre 2023, n. 44154, cit.; sui rapporti tra le prerogative fondamentali *ex* art. 15 Cost. e la tesi che distingue le comunicazioni statiche da quelle dinamiche, v. *funditus,* TROISI, *Le investigazioni digitali sotto copertura,* Bari, 2022, 160 ss. e, più in particolare, 187 ss.

[28] Cort. giust. UE, Grande sezione, 30 aprile 2024, C-178/22.

[29] Cass., Sez. I, 18 gennaio 2024, n. 2312.

tazione, che postula l'apprensione di un flusso comunicativo. Considerare tale tipo di comunicazioni "già concluse" alla stregua di documenti, tuttavia, significa considerarle prove precostituite formatesi al di fuori del procedimento[30].
Ma l'attività di decrittazione, pur ritenuta "genuina" dalla Cassazione in quanto «effettuata facendo ricorso a un algoritmo, il quale esclude la possibilità di manipolazioni o alterazioni dei testi captati», in verità, spesse volte, implica lo svolgimento di ulteriori operazioni che potrebbero «pregiudicare e condizionare la resa conoscitiva, se non svolte nel modo dovuto»[31]. Il che fa ben comprendere come tale attività potrebbe comportare un'ulteriore attività di indagine che mal si concilia con l'impianto della prova documentale.
Ciò trova conferma, peraltro, nell'art. 43, co. 4 d.lgs. 21 giugno 2017, n. 108, che, nel regolare le modalità di intercettazioni di telecomunicazioni con l'assistenza tecnica dell'autorità giudiziaria di altro Stato membro dell'Unione europea, stabilisce che la richiesta contenuta in un OEI possa avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate: lasciando desumere che anche tali attività, per quanto accessorie, se richieste dall'autorità italiana, debbano essere preventivamente autorizzate dal giudice.
Entro tale prospettiva alquanto articolata l'andamento rapsodico seguito dalla giurisprudenza di legittimità risulta avallato dalla frammentarietà normativa e dall'incertezza applicativa in tema di captazioni materiali informatiche.
Posto il ruolo nomofilattico della Corte di cassazione, non può però non tenersi conto che l'affermarsi della giurisdizione delle Corti europee, quale fenomeno chiaramente percettibile della interrelazione tra gli ordinamenti sovranazionali e quello interno, ha ridefinito l'ambito di competenza dei giudici nazionali, determinando «un cambiamento prospettico nella funzione tradizionalmente assegnata alla Corte di cassazione»[32]. Quest'ultima è ora chiamata a garantire un'interpretazione uniforme della legge, riletta alla luce di una complessa dimensione reticolare caratterizzata dall'intersezione di molteplici fonti esterne[33]. Una Corte garante dell'uniformità complessiva dell'interpretazione dell'ordinamento, dunque, la cui attività è sempre più

[30] DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/ Encrochat in attesa delle Sezioni Unite*, in *www.sistemapenale.it*, 11 dicembre 2023.
[31] *Ibidem*.
[32] Cfr. DE AMICIS-VINCENTI-ACIERNO, *Il ruolo della Corte di cassazione: tradizioni e mutamenti*, in *www.cortedicassazione.it*, 2011, 13 ss.
[33] *Ibidem*.

considerata come il punto nodale di un sistema "multilivello" in costante destrutturazione[34] e progressiva ricomposizione.

4. *La presa di posizione delle Sezioni unite*. Al fine di risolvere il conflitto giurisprudenziale fin qui esaminato, sono state rimesse alle Sezioni unite diverse questioni in materia.
In particolare, ci si è chiesti se in tema di mezzi di prova l'acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato, mediante SKY ECC presso autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234-bis c.p.p. o di documenti *ex* art. 234 c.p.p. o, ancora, sia riconducibile ad altra modalità di acquisizione di prove, e se detta acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte dell'autorità giurisdizionale nazionale.
Sono state poste, poi, le seguenti e ulteriori questioni: 1) se l'acquisizione, mediante OEI, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera in un proprio procedimento, su una piattaforma informatica criptata e su criptofonini integri l'ipotesi disciplinata, nell'ordinamento nazionale, dall'art. 270 c.p.p; 2) se, ai fini dell'emissione dell'OEI finalizzato al suddetto trasferimento, occorra la preventiva autorizzazione del giudice; 3) se l'utilizzabilità degli esiti investigativi di cui al precedente punto sia soggetta a vaglio giurisdizionale nello Stato di emissione dell'ordine europeo di indagine.
Le Sezioni unite hanno precisato che 1) il trasferimento all'autorità giudiziaria italiana, in esecuzione di OEI, del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'autorità giudiziaria estera, rientra nell'acquisizione di atti di un altro procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 78 disp. att. c.p.p., 238, 270 c.p.p. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE; 2) che tale trasferimento non deve essere oggetto di verifica giurisdizionale preventiva della sua legittimità nello Stato di emissione dell'ordine europeo di indagine; 3) che l'autorità giurisdizionale dello Stato di

[34] DE AMICIS, *La formulazione del principio di diritto e i rapporti tra Sezioni semplici e Sezioni Unite penali della Corte di cassazione*, in *www.cortedicassazione.it*, 2018.; e ancora sul tema DONINI, *Disposizione e norma nell'ermeneutica penale contemporanea*, in *Europeismo giudiziario e scienza penale,* Milano, 2011, 65 ss.;

emissione dell'OEI deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo.
Nella medesima occasione, le Sezioni unite evidenziavano che l'acquisizione, mediante OEI dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera, in un proprio procedimento, su una piattaforma informatica criptata e su criptofonini integra l'ipotesi, nell'ordinamento nazionale, dell'art. 270 c.p.p. e che, ai fini dell'emissione dell'OEI finalizzato al suddetto trasferimento non occorre l'autorizzazione preventiva del giudice, fermo restando l'obbligo di verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo.
Le motivazioni di dette sentenze, fortemente attese e sopraggiunte di recente, suscitano una serie di riflessioni a cascata, vista l'interdipendenza tra le diverse questioni.
Si focalizzerà l'attenzione su quella che può essere definita la questione prodromica alle altre: l'acquisizione di messaggi scambiati con sistema cifrato mediante piattaforma digitale SKY ECC presso l'autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisce acquisizione di documenti e di dati informatici ai sensi dell'art. 234 *bis* c.p.p.?
Le Sezioni unite considerano non applicabile la disciplina di cui all'art. 234-*bis* c.p.p., rilevando che «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», poiché alternativa e incompatibile rispetto alla disciplina dettata in tema di OEI.
L'art. 234 *bis* c.p.p., disciplinando una modalità di acquisizione di particolari tipologie di elementi di prova presenti all'estero, e non un mezzo di prova, opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie. Ipotesi che, viceversa, viene regolata dall'OEI, il quale disciplina l'acquisizione di elementi di prova "transfrontalieri", realizzata attraverso rapporti di collaborazione tra autorità giudiziarie di Stati diversi. Appare, dunque, evidente la differenza tra acquisizione di elementi istruttori operata direttamente dall'autorità giudiziaria procedente e quella effettuata sulla base di una collaborazione tra diverse autorità giudiziarie.
Tale precisazione mostra di superare l'orientamento precedente della Cassazione che rendeva possibile l'acquisizione della messaggistica, sulla base dell'art. 234 *bis*, propendendo, invece, per l'enfatizzazione della direttiva 2014/41/UE concernente l'OEI, la quale attribuirebbe alla disciplina da essa

dettata una funzione di preminenza e di completezza nell'ambito dei rapporti di collaborazione tra autorità giudiziarie di diversi Stati.
La disciplina dell'OEI, invece, non contiene regole relative alla fase della sua esecuzione volte ad incidere sulla utilizzabilità degli atti nel procedimento davanti all'autorità di ammissione.
Tuttavia, la stessa evidenzierebbe la necessità di assicurare il rispetto dei diritti fondamentali da parte dell'autorità giudiziaria dello Stato di emissione, anche con riguardo alle attività compiute in quello di esecuzione.
Sostanzialmente, in forza del coordinamento normativo tra il decreto legislativo n. 108 del 2017 e la Direttiva 2014/41/UE, ai fini dell'utilizzabilità degli atti acquisiti mediante OEI[35] dall'autorità italiana, è necessario sia garantire i diritti fondamentali dell'Unione europea sia il rispetto delle disposizioni previste dall'ordinamento giuridico in tema di forme ed acquisizione di dati.
Per le Sezioni unite[36], ai fini del rispetto dei diritti fondamentali, assumerebbero rilevanza il principio di presunzione relativa di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera nell'ambito dei rapporti di collaborazione ai fini dell'acquisizione di prove e l'onere per la difesa di allegare e produrre il fatto dal quale dipende la violazione denunciata.
La qualificazione del tipo di atto richiesto è necessaria per valutare la sussistenza delle condizioni di ammissibilità dell'OEI così come la possibilità di disporre l'assunzione dello stesso in un caso interno analogo.
Come evidenziato, nell'ordinamento italiano è previsto che il pubblico ministero possa chiedere ed ottenere la disponibilità di prove già formate in un procedimento penale al fine di produrle in altro procedimento, senza alcuna autorizzazione preventiva da parte del giudice competente per quest'ultimo. Secondo le Sezioni unite, pertanto, sarebbe giustificato il richiamo agli artt. 238, 270 c.p.p. e 78 disp. att. c.p.p. e non sarebbe illegittima la procedura adottata dall'Italia.
Inoltre, la procedura regolamentata dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, concernente l'acquisizione dei dati sul traffico di comunica-

[35] GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine (OEI) per l'acquisizione della digital evidence dal server estero,* in *questa Rivista*, 2023, 3, 6.; ancora sul punto: LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale,* in *Cass. pen.*, 2024, 1, 182 s.
[36] SPANGHER, *Criptofonini: le sentenze delle Sezioni Unite*, in *www.giustiziainsieme.it*, 20 giugno 2024.

zioni elettroniche e la collocazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, non anche alle richieste indirizzate ad altra autorità giudiziaria già in possesso dei dati medesimi.
A puntualizzare il quadro tracciato giunge la sentenza coeva n. 23756 del 2024[37] che, pur riprendendo in larga parte l'*iter* seguito dalla sentenza n. 23755 del 2024, approfondisce un ulteriore aspetto, quello delle intercettazioni estere effettuate attraverso *trojan*[38]: profilo che merita una seppure breve riflessione per i punti d'interferenza con l'argomento trattato.
Poiché il pubblico ministero può disporre l'acquisizione di risultati di intercettazioni ordinate in altro procedimento penale senza la necessità di una preventiva autorizzazione da parte del giudice competente per il procedimento nel quale intende utilizzarli, deve ritenersi che un OEI nel quale si chiede, senza preventiva autorizzazione del giudice nazionale, la trasmissione di risultati di intercettazioni ordinate dall'autorità giudiziaria straniera, abbia ad oggetto atti che avrebbero potuto essere disposti alle medesime condizioni in un caso interno analogo.
Tale conclusione resta la stessa anche se l'operazione di intercettazione sia stata realizzata mediante l'inserimento di un captatore informatico sul *server* della piattaforma di un sistema informatico o telematico, al fine di acquisire le chiavi di cifrature delle comunicazioni. Questo perché non può ritenersi che l'inserimento di un captatore informatico costituisca mezzo atipico di indagine o di prova.
Se da una prima lettura delle risposte offerte dalle Sezioni unite emerge un quadro volto ad avallare la legittimità dell'operato della Procura, d'altro canto non si può prescindere dal considerare il rispetto delle garanzie difensive e i diritti fondamentali nel momento in cui la procedura di acquisizione viene esperita.
Infatti, nella sentenza viene evidenziato che, ai fini dell'utilizzabilità nello Stato di emissione degli atti acquisiti mediante OEI, è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione europea. Tra questi, il diritto di difesa e la garanzia del giusto processo.

---

[37] Cass., Sez. un., 14 giugno 2024, n. 23756, in *www.processopenaleegiustizia.it,* 15 giugno 2024.
[38] V. *amplius,* ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Padova, 2018.

Ciò, secondo la sentenza in parola, come si è visto, sarebbe garantito dal rispetto delle condizioni di ammissibilità dell'OEI e dal fatto che il sistema su cui quest'ultimo si basa sia ispirato al principio di "presunzione relativa" di conformità ai diritti fondamentali delle attività istruttorie svolte dall'autorità giudiziaria degli altri stati dell'Unione[39].

Per quanto, infatti, le Sezioni unite sottolineino l'importanza, ai fini del trasferimento della messaggistica acquisita dall'autorità estera, del rispetto delle condizioni di ammissibilità dell'ordine europeo d'indagine, non si può non sottolineare che la valutazione di tali parametri postula anche la conoscenza delle modalità acquisitive della messaggistica.

Un approccio differente, volto a sorvolare le modalità acquisitive della messagistica, avallerebbe l'automatico recepimento di prove raccolte all'estero di cui non ne è possibile sindacarne l'operato.

Valutare i presupposti di ammissibilità dell'OEI, implica, quindi, un controllo da parte dell'autorità giudiziaria di quelle che sono le modalità acquisitive esperite dalle autorità straniere.

Questo, soprattutto, quando le autorità straniere, per svolgere tali tipo di attività usufruiscano di particolari e complesse strumentazioni volte a decriptare il contenuto della messaggistica.

Le Sezioni unite sembrano superare quest'ultima *impasse* nel momento in cui evidenziano che l'impossibilità per la difesa di conoscere gli algoritmi utilizzati dalle autorità estere per la decriptazione non pare causare, almeno in via di principio, la violazione dei diritti fondamentali; questo perché «il contenuto di ciascun messaggio è sempre abbinato alla sua chiave di cifratura, per cui una chiave errata non avrebbe modo di decriptarlo»[40].

Quest'ultima osservazione lascia un po' perplessi non essendo possibile affidarsi completamente all'intellegibilità delle comunicazioni tramite algoritmi.

La questione afferente alla decrittazione dei messaggi pare, infatti, costituire un punto cruciale in tutte le vicende esaminate, poiché la portata del diritto di difesa, inteso quale uno dei diritti fondamentali da rispettare per poter considerare ammissibile l'OEI, finisce per essere svuotata nel momento in cui si

[39] DANIELE, *Le sentenze "gemelle" delle sezioni unite sui criptofonini*, in *www.sistemapenale.it*, 17 luglio 2024.
[40] *Ibidem.*

ammette una ricezione acritica, nell'ordinamento interno, dei messaggi decriptati, senza possibilità di verifica ad opera delle parti processuali[41].
In particolare, la difesa dovrebbe ottenere la verificabilità delle azioni e dell'algoritmo utilizzato per decrittare la messagistica. È diritto di quest'ultima ripercorrere l'*iter* che ha portato al risultato probatorio, soprattutto nel caso in cui vi sia una possibilità di distorsione del dato originario.
Come autorevolmente rimarcato in dottrina[42], la riproducibilità e verificabilità delle operazioni di decifrazione dei flussi informatici criptati rappresenta un'esigenza difensiva irrinunciabile.
Un sistema basato sull'equo processo non può ammettere una prova «dalla genesi ignota»[43].
In quest'ottica, non sembrerebbe nemmeno congruente il riferimento all'art. 270 c.p.p., la cui *ratio*, come noto, è quella di garantire il diritto costituzionale della libertà di comunicazione e la segretezza delle comunicazioni (art. 15 Cost.), le cui limitazioni sono ammissibili soltanto se poste nel rispetto delle garanzie stabilite *ex lege*. Dunque, ad avviso di chi scrive, dovrebbe ritenersi che la norma *de qua* riguardi pur sempre "altri" procedimenti "interni" all'ordinamento, il cui eventuale *iter* acquisitivo abbia rispettato *ab origine* le garanzie procedurali previste dal nostro codice[44].
E ciò pur dovendosi considerare, per altro verso, l'esistenza del principio del mutuo riconoscimento[45].
In definitiva, la soluzione prospettata presenta criticità che rischiano di depotenziare il rispetto dei diritti fondamentali[46]. La dimensione sovranazionale e i più recenti strumenti tecnologici offrono importanti risorse e opportunità

[41] GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *questa Rivista,* 2024, 1, 6.
[42] Sul punto, ampiamente GAITO, *Comunicazioni criptate,* cit., 9.
[43] FILIPPI, *Criptofonini SKY- ECC e messaggi criptati: la Corte di cassazione attua i principi di diritto enunciati dalle Sezioni Unite*, in *www.penaledp.it*, 11 aprile 2024.
[44] DINACCI, *I modi acquisitivi della messagistica chat o e-mail: verso letture rispettose dei principi*, in *questa Rivista,* 2024, 1, 19.
[45] Sul tema: SCALFATI, *Note minima cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. giust.*, 2017, 2, 217. VALENTINI, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, 1998; UBERTIS, *La prova acquisita all'estero e la sua utilizzabilità in Italia*, in *Cass. pen.*, 2014, 2, 696; TRIPICCIONE, *Il regime di utilizzabilità della prova digitale formata all'estero ed acquisita tramite ordine europeo di indagine*, in *Cass. pen.*, 2024, 2, 692.
[46] Sul punto, v. CONTI, *Il principio di non sostituibilità: il sistema probatorio tra costituzione e legge ordinaria*, in *Cass. pen.*, 2024, 2, 452; SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*, in *Cass. pen.*, 2024, 1, 173.

all'attività investigativa, tuttavia, sia il contesto sovranazionale sia il divenire tecnologico, devono pur sempre confrontarsi, con gli *standard* di tutela assicurati dall'ordinamento nazionale, per far si che quelle garanzie proprie del processo penale, come il diritto di difesa e tutte le altre situazioni giuridiche soggettive interdipendenti e costituzionalmente riconosciute, siano considerati non meri ornamenti, ma fulcro di un sistema garantista.

Nel bilanciamento tra valori in gioco, i principi del giusto processo devono continuare a fornire le coordinate di riferimento delle dinamiche procedimentali che incidono sulle libertà inviolabili della persona umana e che rappresentano "controlimiti" invalicabili anche per il diritto dell'Unione europea.