# ANCORA IN TEMA DI CRIPTOFONINI: NUOVI ARRESTI GIURISPRUDENZIALI IN ATTESA DELLE SEZIONI UNITE

*Wanda Nocerino*

*Cass., Sez. VI, 26 ottobre 2023, n. 44154; Cass., Sez. VI, 26 ottobre 2023, n. 44155*

**1. Criptofonini e prova penale: un rapporto in continua evoluzione**

Troppo ingenuamente si è pensato che il fermento giurisprudenziale sui criptofonini si fosse arrestato in ragione delle granitiche posizioni dei giudici di legittimità[1] che, nel delineare il regime di utilizzabilità della messaggistica scambiata su sistema cifrato *Sky Ecc* ed *Encrochat*, hanno chiarito che l'acquisizione dei dati

decriptati e conservati all'estero non soggiace alle regole previste in materia di intercettazioni informatiche o telematiche, *ex* art. 266-*bis* c.p.p., trovando invece applicazione il dettato di cui all'art. 234-*bis* c.p.p.

Discostandosi (almeno apparentemente) dai precedenti indirizzi, la Corte –con due pronunce "gemelle"[2] – precisa che la qualificazione giuridica delle investigazioni svolte all'estero sulle piattaforme criptate dipende dal tipo di atto condotto e, dunque, varia in base all'oggetto e alle modalità acquisitive dell'elemento probatorio, oscillando tra la categoria delle intercettazioni telematiche e quella dei sequestri presso gli *Internet Service Providers*.

Nell'occasione, i giudici si soffermano anche sulla verifica della sussistenza delle condizioni per l'emissione dell'Ordine Europeo di Indagine (OEI) al fine di acquisire prove in territorio unionale e sulla legittimazione del p.m. ad autorizzare l'acquisizione di "documenti" informatici all'estero, riscontrando un'aporia sistemica laddove per l'apprensione dei dati esterni del traffico telefonico e telematico (c.d. tabulati), il d.l. n. 132 del 2021 richiede l'intervento preventivo dell'organo giurisdizionale.

Già da questa prima ricostruzione dello stato dell'arte, emerge la complessità delle questioni che la giurisprudenza si trova ad affrontare: da una parte, si profilano criticità di natura classificatoria, determinate dalla difficoltà di individuare la categoria probatoria in cui ascrivere le attività espletate su tali sistemi e, di conseguenza, emergono dubbi circa la diagnosi di utilizzabilità processuale dei dati ottenuti a seguito di decriptazione dei dati giacenti sui *server*; dall'altra, si tratta di comprendere se e a quali condizioni sia legittimo il ricorso all'OEI per acquisire dati e documenti informatici raccolti all'estero, posto che non sempre l'atto di indagine richiesto nell'ordine è svolto nelle medesime forme previste dalla normativa interna.

Senza voler anticipare le riflessioni che verranno svolte nel prosieguo, conviene partire da un assunto difficilmente confutabile: i profili differenziali della tecnica investigativa in esame rispetto alle categorie probatorie "tradizionali" rendono complessa l'opera di sussunzione delle attività esperite sulle piattaforme criptate nell'alveo dei mezzi di ricerca della prova già noti al sistema. Eppure, non potendo arrendersi all'idea che le nuove indagini finiscano per rimanere improficue a causa di una normativa non sempre al passo con i tempi, il giurista – proprio come è accaduto quando il processo penale si è trovato al cospetto del captatore informatico[3] e dell'*IMSI Catcher*[4] – deve compiere uno sforzo ermeneutico per adeguare, nel rispetto dei principi dell'ordinamento giuridico, la disciplina vigente alle nuove sfide dell'era moderna[5].

**2. Un *revirement* solo apparente**

Prima ancora di analizzare il contenuto delle pronunce in commento, occorre soffermarsi brevemente sul caso di specie da cui le stesse traggono origine.

Pur non essendo ufficialmente noti i singoli passaggi investigativi che hanno portato all'apprensione degli elementi di prova mediante accesso ai *server* della società canadese (*Sky Global*) di *Sky Ecc*, è dato sapere che l'indagine si è sviluppata con l'istituzione di una squadra investigativa comune, composta dalle autorità giudiziarie e da rappresentanti delle forze di polizia di Belgio, Francia e Olanda, che ha operato con il supporto di *Eurojust* ed *Europol.*

Materialmente, l'acquisizione del contenuto della messaggistica è avvenuta per il tramite delle autorità francesi – luogo in cui il *server* della società di *Sky Ecc* è ubicato – secondo la previsione dell'art. 706-102-1 del *code de procédure pénale* che consente di accedere, conservare, registrare e trasmettere dati archiviati su sistemi informatici.

L'operazione non è rimasta confinata ai Paesi direttamente interessati dall'indagine: infatti, in diversi procedimenti penali nazionali è emersa la necessità di acquisire, mediante OEI, i dati comunicativi ritenuti di interesse per l'accertamento dei reati perseguiti nei singoli procedimenti. L'acquisizione di tali dati ha determinato una sequela di provvedimenti cautelari che, a cascata, hanno generato altrettante pronunce della Corte di Cassazione.

In un simile contesto, i giudici di legittimità vengono chiamati a decidere *in primis* sui limiti di impiego processuale dei contenuti della messaggistica scambiata per il tramite di criptofonini procacciati dalle forze di polizia di altri Stati europei e acquisiti per il tramite dell'ordine.

Per risolvere l'enigma, la Corte parte dal "dato tecnico", individuando le singole attività di indagine condotte dall'autorità giudiziaria estera: per la prima volta, dopo il silenzio serbato nei precedenti giurisprudenziali, i giudici ammettono che, oltre a raccogliere dati "freddi" precostituiti, gli inquirenti francesi – una volta avviato il procedimento penale – hanno acquisito le *chat* e la messaggistica giacente sui *server* e appreso i flussi di comunicazione in transito avviato tra i fruitori del servizio.

A parere dei giudici, quindi, non è sempre possibile applicare il dettato di cui all'art. 234-*bis* c.p.p., posto che il

ricorso alla norma in esame può ritenersi giustificato esclusivamente nell'ipotesi di acquisizione di dati e documenti informatici – intesi come elementi informativi "dematerializzati" – che preesistono rispetto all'avvio delle indagini. In quest'ottica, qualora l'attività investigativa si concretizzi nell'apprensione occulta del contenuto archiviato nel *server* nel corso dell'investigazione, la relativa acquisizione va inquadrata nella disposizione di cui all'art. 254-*bis* c.p.p.; qualora, poi, l'attività consista nella captazione e registrazione del messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, il mezzo di ricerca della prova più congeniale è quello dell'intercettazione telematica, *ex* art. 266-*bis* c.p.p.[6].

Ciò significa che l'inquadramento normativo delle investigazioni sulle piattaforme criptate non può essere "standardizzato" e va inteso come "relativo", mutando di volta in volta in base al tipo di attività per cui viene concessa l'autorizzazione a procedere.

Se così stanno le cose, allora deve rilevarsi che la posizione della Corte non sembra poi così difforme dagli arresti precedenti: a ben guardare, infatti, la giurisprudenza di legittimità non ha mai escluso *tout court* la possibilità di sussumere l'attività investigativa nel novero delle intercettazioni telematiche o del sequestro, *ex* art. 254-*bis* c.p.p.[7]. Certo è che se fino a questo momento nelle diverse ordinanze impugnate non veniva fatto cenno alle altre attività – diverse ed ultronee dall'acquisizione di dati formati prima ed indipendentemente dall'avvio delle indagini sul territorio nazionale –, i giudici non avrebbero potuto intravedere nessun'altra copertura normativa se non quella fornita dall'art. 234-*bis* c.p.p.

Al di là delle questioni legate alla natura dell'attività acquisitiva e del relativo mezzo di ricerca della prova in cui ascrivere l'investigazione, la Corte si sofferma anche su un altro aspetto, relativo alla legittimità dell'emissione dell'OEI per raccogliere gli elementi di prova raccolti all'estero.

Intanto, posta l'esistenza del c.d. "principio di equivalenza" – 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 dall'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo», *ex* art. 6, par. 1, lett. *b,* Direttiva 2014/41/UE –, i giudici rilevano l'impossibilità di procedere a investigazioni transfrontaliere disattendendo le regole di ammissibilità della prova riconosciute dall'ordinamento nazionale. Di conseguenza, gli elementi probatori raccolti devono essere ritenuti inutilizzabili perché acquisiti in violazione del diritto di difesa e delle regole del contraddittorio[8]. Non va, infatti, dimenticato che, pur non potendo pretendere un integrale adattamento della fattispecie tipica dell'atto rogato alle linee del modello processuale interno, «le prerogative difensive […] non possono essere compresse nel loro nucleo

essenziale»[9]: in questo caso, secondo i giudici, il diritto dell'imputato di conoscere e contestare il materiale probatorio utilizzato a proprio carico risulta violato nella parte in cui alla difesa non viene consentita la possibilità di verificare la piena corrispondenza tra il testo originario (ossia la stringa informatica) e il testo intelligibile introdotto come prova nel giudizio[10].

Sempre in rapporto alla legittimità dell'OEI, la Corte si sofferma anche su una questione mai esplorata nei precedenti casi affrontati dalla giurisprudenza. Ci si riferisce alla legittimazione della procura ad emettere l'ordine durante la fase investigativa e all'assenza di una qualsivoglia forma di "intermediazione" del giudicante che, come noto, non interviene ad eccezione del caso in cui la richiesta abbia ad oggetto un'attività intercettiva.

In questo caso, secondo i giudici, si realizza un "cortocircuito" sistemico laddove per l'acquisizione dei tabulati telefonici è richiesto l'intervento del giudicante (d.l. 132/2021) nel rispetto della riserva di giurisdizione: dunque, «l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione [deve] essere sempre autorizzata da un giudice [perché] sarebbe davvero singolare che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del p.m.»[11].

**3. La natura delle investigazioni sulle piattaforme criptate**

Come si è avuto di anticipare, il più complesso problema da risolvere è la tassonomia probatoria in cui ascrivere le attività di indagine esperite sulle piattaforme criptate. Convenendo con l'impostazione metodologica seguita dalla Corte, si ritiene che la qualificazione giuridica delle attività esperite sulle piattaforme criptate sia strettamente interconnessa al tipo di dati oggetto di *adprehensio* e al "momento" in cui questa si realizza, dovendosi distinguere a seconda che l'acquisizione abbia ad oggetto dati precostituiti all'avvio del procedimento ovvero dati che si sono formati nell'ambito di iniziative istruttorie in atto.

Intanto, occorre verificare se l'acquisizione di comunicazioni avvenga contestualmente alla trasmissione dell'informazione ovvero in un momento successivo allo scambio comunicativo.

Circoscrivendo l'analisi al caso in cui l'azione acquisitiva sia "*live*" – e, dunque, la captazione avvenga nel

momento in cui la comunicazione transita nell'etere digitale –, la categoria probatoria con cui sembra opportuno confrontarsi è rappresentata dalle intercettazioni telematiche, regolate dall'art. 266-*bis* c.p.p.

Sicuramente, sotto il profilo tecnico-operativo, l'accesso ad un *server* per captare comunicazioni in atto può essere ricompreso nell'alveo delle intercettazioni telematiche, venendo in rilievo il carattere della contestualità della captazione di un flusso comunicativo tra sistemi collegati in Rete.

Tuttavia, pur volendo assimilare tali forme captative alle intercettazioni "classiche", non si può negare che le prime siano caratterizzate da significative peculiarità, risultando molto più intrusive per chi vi è sottoposto e, al contempo, assai più efficaci per i loro esiti istruttori.

Si converrà che un conto è captare flussi telematici intercorrenti tra due o più sistemi oggetto di intercettazione, ben altro è accedere direttamente al *server* sul quale transitano tutte le comunicazioni di tutti gli utenti che utilizzano quel servizio. Di qui, si potrebbe dubitare del fatto che tali attività possano essere sussunte nella disciplina di cui all'art. 266-*bis* c.p.p., che, come precisato, «consente limitazioni mirate»[12], circoscrivendo l'ambito della captazione nel pieno rispetto dei *dicta* costituzionali e convenzionali[13].

Se questa è un'eccezione condivisibile, sembra possibile un'interpretazione "evolutiva" del dettato normativo, peraltro suggerita dalla giurisprudenza della Corte EDU, per cui «deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta»[14]. E, allora, così ragionando, il *server* potrebbe essere considerato come un contenitore (*rectius:* spazio) su cui transitano flussi comunicativi da attenzionare, non dissimile dallo *smartphone* o dal *computer*.

Si potrebbe, in altri termini, arrivare ad affermare che tale captazione rappresenti un'evoluzione dell'intercettazione telematica "tradizionale" avendo ad oggetto flussi comunicativi transitanti su un nuovo "sistema informatico", ossia il *server*, posto che è proprio quello spazio a dover essere "monitorato" perché è sul nuovo ambiente virtuale che (presumibilmente) si consuma il fatto di reato.

L'approccio è parzialmente difforme nel caso in cui gli investigatori acquisiscano dati informatici "freddi" dal contenuto comunicativo[15]. In questo caso, occorre distinguere a seconda che l'apprensione abbia ad oggetto dati precostituiti (ossia formati al di fuori del procedimento), ovvero dati giacenti sul *server*.

Tradizionalmente, come chiarito dalla giurisprudenza di legittimità[16], i messaggi conservati nella memoria di un cellulare devono essere considerati documenti, ai sensi dell'art. 234 c.p.p., posto che gli stessi «non rientrano nel concetto di "corrispondenza", in quanto quest'ultima implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito [...]»; e nemmeno può ritenersi che si tratti degli esiti di un'attività di intercettazione «la quale postula, per sua natura, la captazione di un flusso di comunicazioni in atto. [...] i dati presenti sulla memoria del telefono acquisiti *ex post* costituiscono mera documentazione di detti flussi»[17].

Di conseguenza, non può dubitarsi del fatto che i messaggi decriptati rientrino nel novero dei documenti informatici dal contenuto comunicativo, trattandosi di «rappresentazioni comunicative incorporate su base materiale con metodo digitale»[18]. Dunque, allorquando si procede ad acquisire dati informatici che preesistono rispetto al momento dell'avvio delle indagini, il relativo atto investigativo non può che soggiacere alla disciplina di cui all'art. 234-*bis* c.p.p. che, come noto, consente l'acquisizione di documenti e dati informatici conservati all'estero, previo consenso del legittimo titolare.

Allorquando, però, si procede ad acquisire dati informatici dal contenuto comunicativo archiviati nel *server* nell'ambito di un procedimento penale, la relativa attività di indagine non può che avvenire secondo le previsioni di cui all'art. 254-*bis* c.p.p., riguardante le ipotesi di sequestro presso fornitori di servizi informatici, telematici e di comunicazioni.

Deve, tuttavia, evidenziarsi che anche tale procedura sussuntiva non è scevra da criticità. Come noto, infatti, il decreto di sequestro deve contenere una specifica motivazione sulla finalità perseguita per l'accertamento dei fatti[19] e deve essere finalizzato all'apprensione solo di quanto sia effettivamente utile ai fini di indagine[20], nel pieno rispetto del principio di proporzionalità[21]. Tuttavia, in alcune pronunce, la Corte di legittimità esclude la violazione del principio di proporzionalità laddove il sequestro dell'intero contenuto di un sistema informatico sia necessitato da specifiche esigenze probatorie che vengono in rilievo sulla base delle peculiarità del fatto di reato per il quale si procede[22].

Di conseguenza, non sussisterebbero ragioni ostative all'acquisizione del contenuto informativo giacente sul *server* allorquando il decreto che dispone la misura contenga la precisa indicazione delle ragioni che giustificano l'estensione dell'apprensione, in modo tale da consentire un controllo postumo sulla proporzionalità del vincolo apposto sui dati informatici.

**4. La legittimità dell'OEI**

L'altro aspetto sul quale si canalizza l'attenzione dalla Corte inerisce alla legittimità dell'emissione dell'OEI quale strumento di cooperazione investigativa da impiegare per acquisire gli elementi di prova raccolti in un territorio eurounitario.

In primo luogo, occorre interrogarsi sull'opportunità (*rectius:* necessità) di formulare un rinvio pregiudiziale alla Corte di Giustizia circa la possibilità di ricorrere all'OEI in situazioni analoghe a quelle prospettate nel caso di specie: sulla scia di quanto accaduto con la decisione *HP* del 16 dicembre 2021, C-724/19[23], i giudici di Lussemburgo potrebbero fare chiarezza sui limiti di impiego dello strumento cooperativo per ottenere elementi di prova (nella specie documenti dal contenuto comunicativo) acquisiti all'estero seguendo regole diverse da quelle previste dall'ordinamento interno e senza l'autorizzazione dell'organo giurisdizionale. In tale ottica, qualora la Corte propendesse per l'impossibilità di ricorrere all'OEI, il materiale probatorio tradotto in Italia dovrebbe essere affetto da inutilizzabilità, determinando un effetto domino che finisce per travolgere le questioni procedurali interne.

In secondo luogo, come anche osservato dalla Corte, il ricorso all'ordine potrebbe profilare alcune criticità in rapporto al principio di legalità della prova, al quale il sistema della cooperazione transfrontaliera è informato: infatti, sia l'art. 1, § 4 della direttiva 2014/41/UE che l'art. 1, d.lgs. 108/2017 sanciscono il dovere di rispettare i principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione Europea. Inoltre, pur rimettendo alle scelte dei singoli Stati la valutazione probatoria degli elementi investigativi raccolti all'estero[24], nell'articolato legislativo sono previste – più o meno esplicitamente – regole di esclusione delle prove acquisite *contra legem.* Solo a titolo esplicativo, si pensi all'art. 6, § 1 della direttiva, trasposto nell'art. 27 del decreto in rapporto all'inutilizzabilità delle prove acquisite in violazione dei requisiti nazionali di ammissibilità, all'art. 9, § 2 della direttiva, trasfuso nell'art. 4, commi 2, 3 e 5 del decreto in rapporto alle prove acquisite violando le norme sul *quomodo* delle attività istruttorie, all'art. 36 del decreto in rapporto all'inutilizzabilità per l'inosservanza delle garanzie difensive.

Senza entrare nel merito dei rimedi esperibili contro le violazioni dei diritti fondamentali, dall'esegesi delle norme che tipizzano le *exclusionary rules* si ricava un principio generale di diritto consistente nell'impossibilità di procedere ad investigazioni transfrontaliere per l'acquisizione di elementi probatori utili alle indagini disattendendo le regole di ammissibilità delle prove operanti a livello nazionale, pena l'inutilizzabilità delle informazioni raccolte[25].

In altre parole, allo stato attuale, spetta al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati, contraria al diritto dell'Unione (c.d. principio di autonomia procedurale).

Di qui, si potrebbe arrivare a ritenere che i risultati di indagini esperite all'estero e acquisiti in Italia per il tramite dell'OEI sarebbero inutilizzabili perché ottenuti disattendendo le regole nazionali sul diritto di difesa e sul contraddittorio nella formazione della prova che, come noto, impongono all'autorità inquirente di disvelare tutte le prove e tutto quanto sia necessario per dimostrare la regolarità delle procedure di acquisizione degli elementi di prova, soprattutto nella dimensione digitale[26].

L'assunto non sempre del tutto convincente: intanto, se è vero che il diritto di difesa risulta frustrato dalla scelta della procura di mettere a disposizione i soli esiti dell'attività svolta all'estero e non anche il percorso di acquisizione di quei dati[27], è altrettanto vero che l'autorità giudiziaria estera si è resa garante del rispetto delle corrette procedure acquisitive del dato informatico volte ad impedirne l'alterazione, esistendo una presunzione – invero solo relativa[28] – di legittimità dell'atto di indagine compiuto all'estero.

Inoltre, va sottolineato che il fondamentale diritto di difesa (e con esso il principio del contraddittorio nella formazione della prova) non trova tutela assoluta, potendo ritenersi indispensabile un bilanciamento con interessi concorrenti tra i quali la sicurezza nazionale o la necessità di mantenere segreti specifici metodi e tecniche di indagine[29].

Di conseguenza, nel caso di specie, pur se non vengono disvelati tutti gli elementi di prova sui quali si sono fondate le singole ordinanze cautelari, non si intravede una violazione del diritto di difesa e del contraddittorio, posto che le esigenze di sicurezza (inter)nazionale giustificano l'apposizione del segreto di Stato da parte dell'autorità francese e, dunque, il riserbo su alcune procedure operative da parte dell'autorità italiana.

Assai più rilevante appare la questione relativa alla possibilità di legittimare l'organo del p.m. ad autorizzare l'acquisizione di dati informatici all'estero.

Come è noto, l'art. 27 della Direttiva stabilisce che le autorità competenti a emettere l'OEI sono il p.m. e il giudice che procede nell'ambito delle rispettive attribuzioni, assegnando al primo – ad eccezione del caso in cui l'atto da acquisire all'estero abbia ad oggetto le intercettazioni – la legittimazione ad emettere l'ordine senza preventiva autorizzazione del giudicante.

Nel caso di specie, pur se l'atto investigativo non rientra sempre nel novero delle intercettazioni, si tratta di acquisire all'estero documenti e dati informatici inerenti alla corrispondenza[30] e, dunque, di attività che determinano una compressione del diritto di cui all'art. 15 Cost., giustificabile solo nel rispetto della riserva di legge e di giurisdizione.

Di conseguenza, concordando con la posizione assunta dalla Corte, ogni attività di indagine che si spinga fino all'apprensione di dati dal contenuto comunicativo all'estero dovrebbe essere sempre autorizzata da un giudice, anche in considerazione delle scelte sistemiche effettuate dal legislatore (d.l. n. 132 del 2021) per cui l'acquisizione dei dati esterni del traffico telefonico e telematico (c.d. tabulati), richiede l'intervento preventivo dell'organo giurisdizionale.

**5. Prospettive *de jure condendo***

Alla luce delle ricostruzioni offerte, possono trarsi alcune considerazioni che offrono nuovi spunti di riflessione all'alba di una nuova era che le investigazioni sulle piattaforme si accingono a sperimentare. Il riferimento corre alla prossima pronuncia delle Sezioni Unite – sollecitate dalla III Sezione all'indomani del deposito delle pronunce in commento – chiamate a dirimere un duplice contrasto, ossia «[S]e, in tema di mezzi di prova, la acquisizione mediante OEI di messaggi su *chat* di gruppo presso l'autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca o meno acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* c.p.p.» e «[S]e [...] 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 dell'autorità giudiziaria nazionale».

Per come posti, i quesiti non sembrano idonei a sortire gli effetti sperati, ponendo l'accento solo su alcuni dei complessi aspetti che involgono il tema delle indagini sulle piattaforme criptate; di conseguenza, lungi dal voler pronosticare quanto accadrà nell'imminente futuro, si ha la sensazione che le risposte (a rime obbligate) della Corte potranno risolvere solo in parte le criticità evidenziate.

In rapporto al primo quesito, deve evidenziarsi che non possono esistere risposte univoche. Non è possibile cristallizzare l'acquisizione di dati comunicativi all'estero nell'alveo di un singolo mezzo di ricerca della prova, dovendo far riferimento, di volta in volta, alla *species* di attività compiuta, all'oggetto dell'apprensione e al momento procedurale in cui l'atto viene esperito.

Di qui, l'acquisizione di dati informatici dal contenuto comunicativo acquisiti all'estero è un'attività perennemente in bilico tra differenti istituti processuali, quali le intercettazioni di flussi telematici (art. 266-*bis* c.p.p.), il sequestro di dati informatici presso gli *Internet Service Providers* (art. 254-*bis* c.p.p.), ovvero una prova documentale nel caso in cui l'*adprehensio* abbia ad oggetto dati precostituiti (art. 234 *bis* c.p.p.).

Con riferimento al secondo quesito, va rilevato che – trattandosi di acquisizione all'estero di documenti e dati informatici inerenti alla corrispondenza o altra forma di comunicazione – sarebbe indispensabile prevedere un "controllo" giurisdizionale (preventivo o postumo) per garantire il pieno rispetto della riserva di giurisdizione di cui all'art. 15 Cost.

Tuttavia, una simile scelta di campo esula dalle competenze della giurisprudenza di legittimità, travalicando le sue stesse funzioni: in tale caso, infatti, si rende necessario l'intervento del legislatore nell'ottica di riportare coerenza all'interno del sistema attraverso la giurisdizionalizzazione della procedura di acquisizione dei dati e dei documenti dal contenuto comunicativo.

Di conseguenza, sarebbe maggiormente auspicabile un intervento legislativo volto ad introdurre – al pari di quanto accaduto in altri Paesi europei[31] – un nuovo mezzo di ricerca della prova (accesso e acquisizione di *big data* su sistemi informatici o telematici, potrebbe chiamarsi) per regolare le attività di accesso, osservazione e acquisizione di dati e informazioni rinvenuti sui nuovi spazi virtuali: in questi casi, non sarebbe tipizzato lo strumento con cui condurre le indagini informatiche quanto piuttosto le regole cui ricorrere ogni qual volta si proceda ad attività di sorveglianza occulta e continuativa da remoto, predisponendo le garanzie fondamentali che devono essere sempre riconosciute all'indagato e ai soggetti terzi occasionalmente coinvolti, a prescindere dalla tecnica investigativa impiegata.

In altre parole, l'obiettivo potrebbe essere quello di introdurre una nuova categoria probatoria, con la quale verrebbero individuati i "casi" e i "modi" dell'ingerenza nella sfera privata degli individui, così da ritenere il sacrificio dei diritti inviolabili assolutamente rispettoso del principio di stretta legalità e del principio di proporzione.

[1] Cass., Sez. IV, 5 aprile 2023, n. 16347, in *questa Rivista*; Cass., Sez. I, 13 gennaio 2023, n. 19082, in *CED Cass.,* n. 284440; Cass., Sez. IV, 15 luglio 2022, n. 32915, in *Giur. pen.*, con nota di Barbieri, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine;* Cass., Sez. I, 13 ottobre 2022, n. 6363, in *Cass. pen.,* 2023, 2786, con nota di Nocerino, *L'acquisizione della messaggistica su sistema criptati: intercettazioni o prova documentale?*; Cass., Sez. I, 1 luglio 2022, n. 34059, non massimata.

[2] Cass., Sez. VI, 26 ottobre 2023, n. 44154, non massimata; Cass., Sez. VI, 26 ottobre 2023, n. 44155, non massimata. Per un primo commento, si rinvia a Spangher, Chat. *Saranno le Sezioni Unite a "decriptare" le questioni giuridiche,* in *Giust. insieme,* 13 novembre 2023; Resta, *Criptofonini e ordine europeo di indagine: le questioni poste alle Sezioni Unite, ivi,* 16 novembre 2023.

[3] Sul punto, si consenta un rinvio a Nocerino, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova, 2021.

[4] Per approfondimenti, Camon, *Il cacciatore di* IMSI, in *Arch. pen.*, 2020, f. 1, 1 ss.

[5] Come osserva Torre, WhatsApp *e l'acquisizione processuale della messaggistica istantanea*, in *Dir. pen. proc.*, 2020, 1279, «[...] l'esponenziale sviluppo tecnologico nel campo delle comunicazioni rende sempre più difficile il lavoro dell'interprete, il quale, nel tentativo di sussumere una determinata attività processuale nelle fattispecie astratte, ha a disposizione un quadro obsoleto». Rileva la necessità di adeguare le categorie esistenti con il progresso tecnico-scientifico, Tonini, *L'evoluzione delle categorie tradizionali: il documento informatico*, in Cybercrime*. Trattato di diritto penale*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 1506.

[6] Tale differenza è stata sottolineata, tra le altre, anche da Cass., Sez. IV, 15 ottobre 2019, n. 49896, in *CED Cass.*, n. 277949; Cass., Sez. III, 26 settembre 2019, n. 47557, *ivi*, n. 277990.

[7] Cass., Sez. IV, 5 aprile 2023, n. 16347, cit.; Cass., Sez. I, 1 luglio 2022, n. 34059, cit.; Cass., Sez. I, 13 ottobre 2022, n. 6363, cit.

[8] In una isolata pronuncia (Cass., Sez. IV, 15 luglio 2022, n. 32915, cit.), la Corte ha sostenuto che l'acquisizione del dato probatorio (le *chat* decriptate) è inutilizzabile poiché non è stato rispettato il diritto di difesa. Precisamente, la Cassazione afferma che il principio del contraddittorio implica una dialettica procedimentale non solo sugli esiti del materiale acquisito, ma anche sulle modalità con cui è stato acquisito detto materiale. Ne consegue che, *ex* art. 191 c.p.p., una prova è inutilizzabile se viola i divieti stabiliti dalla legge. In conclusione, per i giudici di legittimità, la difesa gode del diritto di accedere alla documentazione dell'attività investigativa svolta e di conoscere le modalità con cui erano state acquisite tali messaggi criptati, in virtù dell'osservanza del diritto di difesa e di contraddittorio.

[9] Cass., Sez. VI, 26 ottobre 2023, n. 44154, cit., 18.

[10] Conforme a Sez. IV, 5 aprile 2023, n. 16347, cit.

[11] Cass., Sez. VI, 26 ottobre 2023, n. 44154, cit., 9.

[12] Così Filippi,sub *art. 266* bis, in AA. VV., *Codice di procedura penale commentato,* a cura di Giarda- Spangher, Milano-Padova, 2023.

[13] Sul punto, per tutti, Bargi, *L'elusione delle garanzie sostanziali convenzionali nella riforma delle intercettazioni tra illusione (la tutela della privacy) e realtà,* in AA. VV., *Regole europee e processo penale*, a cura di Gaito-Chinnici, 2018, Milano-Padova, 2018, 87 ss.

[14] Sul punto Corte EDU, 4 dicembre 2015, *Roman Zakharov c. Russia*.

[15] Secondo il significato attribuito da Corte cost., 27 luglio 2023, n. 170, «[P]osta elettronica e messaggi inviati tramite l'applicazione *WhatsApp* (appartenente ai sistemi di cosiddetta messaggistica istantanea) rientrano [...] a pieno titolo nella sfera di protezione dell'art. 15 Cost., apparendo del tutto assimilabili a lettere o biglietti chiusi».

[16] Cass., Sez. VI, 6 febbraio 2020, n. 12975, in *CED. Cass.,* 278808;Cass., Sez. VI, 28 maggio 2019, n. 28269, *ivi,*

n. 276227.

[17] Così Cass., Sez. I, 2 dicembre 2020, n. 461, in *Sist. pen.,* 29 marzo 2021. Delineano l'acquisizione della messaggistica istantanea quale sequestro di documenti informatici, *ex plurimis,* Cass., Sez. V, 7 ottobre 2021, n. 3591, in *Cass. pen.* 2022, 3106, con nota di Procaccino, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche. Contra* Corte cost., 27 luglio 2023, n. 170, cit., per cui «[D]egradare 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».

[18] Tonini, *L'evoluzione delle categorie tradizionali: il documento informatico*, cit., 1507.

[19] Cfr. Cass. Sez. Un., 19 aprile 2018, n. 36072, in *Proc. pen. giust.,* 2019, con nota di Cortesi, *Sequestro del corpo del reato e onere motivazionale: dopo un tormentato dibattito interpretativo raggiunto "forse" un punto fermo*.

[20] In questo senso, Caianiello, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont.,* 18 giugno 2014.

[21] Sul punto, più di recente, Algeri, *Principio di proporzionalità e sequestro probatorio di sistemi informatici,* in *Dir. pen. proc.,* 2020, 850; Cascone, *Il sequestro informatico nel prisma del principio di proporzione, ivi,* 2022, 123.

[22] In questo senso, Cass., Sez. Un., 20 luglio 2017, n. 40963, in *Cass. pen.,* 2018, 131.

[23] Sul punto, per tutti, Daniele, *Il controllo giurisdizionale sull'emissione dell'ordine europeo di indagine: la necessaria simmetria con la disciplina nazionale nei casi interni analoghi*, in *Sist. pen*., 31 marzo 2022.

[24] Ai sensi dell'art. 14, § 7, «[...]. 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».

[25] In sostanza, l'OEI deve avere ad oggetto una prova acquisibile nello Stato di emissione e deve essere eseguito in conformità di quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria, potendosi peraltro presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario. Cfr. Cass., Sez. VI, 25 ottobre 2022, n. 48330, in *CED Cass.*, n. 284027.

[26] Cass., Sez. VI, 21 settembre 2023, n. 38678, in *questa Rivista,* 4 ottobre 2023, con nota di Cecchi, *Ancora una pronuncia di legittimità sull'utilizzabilità, come prova documentale, dei messaggi estrapolati da dispositivi mobili*.

[27] Sul punto, Filippi, *Criptofonini e diritto di difesa,* in *questa Rivista,* 2023, 2, 321; Ludovici, *I criptofonini: sistemi informatici criptati e* server *occulti, ivi,* 14 ottobre 2023.

[28] Cfr. Morcella, *La vicenda dei criptofonini in attesa della decisione della Cassazione,* in *Ius,* 6 aprile 2023.

[29] CEDU, Grande Camera, 26 settembre 2023, *Yüksel Yalcinkaya c. Turchia*.

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

[31] Cfr. art. 706-102-1 del *code de procédure pénale* francese.