LA VICENDA DEI CRIPTOFONINI: LE QUESTIONI APERTE IN ATTESA DELL'IMMINENTE INTERVENTO DELLE SEZIONI UNITE

Giulia Fiorucci

Sommario: 1. La vicenda – 2. Nel tentativo di comprendere le attività svolte... – 3. ...Un rapido sguardo al contenuto degli Ordini europei di indagine – 4. Precarie conclusioni

1 - La vicenda

Quando diritto e tecnologia si incontrano, i nodi da sciogliere diventano quasi sempre “doppi nodi”. Questo perché la natura delle due discipline è – per molti aspetti – incompatibile. L’una rapida e in continuo movimento, l’altro variabile, ma con tempi e modi decisamente “lenti” sono sempre più di frequente – considerando lo sviluppo e l’innovazione digitale – a contatto, dovendo affrontare e risolvere problemi comuni.

È il caso della vicenda che vede protagonista la società di telecomunicazioni canadese, Sky Global, fornitrice di criptofonini, attraverso i quali numerosi soggetti – alcuni di questi indagati perché appartenenti alla criminalità organizzata – riuscivano a conversare mediante la piattaforma Sky ECC, piattaforma di messaggistica crittografata. La lunga e complessa indagine, quasi contemporanea e, comunque, simile a quella di Encrochat – condivisa da diversi paesi europei – si è concentrata sull’acquisizione delle *chat* e dei messaggi criptati in parte contenuti nei singoli criptofonini, in parte conservati nel *server* in cui transitavano le *chat*. Di difficile comprensione – almeno per ora – è la modalità investigativa. Secondo quanto è possibile comprendere dalla lettura fornita dai magistrati nostrani, le indagini sono state svolte dai cugini d’oltralpe considerato anche che il *server* ora nominato si trovava in territorio francese. Gli investigatori avrebbero installato un *trojan* in grado di copiare e trasmettere a un *server* della Gendarmeria tutte le *chat* confluite sul *server* della piattaforma Sky ECC, grazie all’autorizzazione emessa dal giudice francese competente; autorizzazione che si è dovuta rinnovare a causa della scoperta da parte della Sky ECC di una falla nel sistema con conseguente aggiornamento della sicurezza. Oltre alle *chat*, questa attività avrebbe permesso anche di acquisire le chiavi di cifratura – necessarie a decriptare i messaggi che, seppur acquisiti, continuavano a non poter essere letti – presenti nel *server*. A quanto pare, però, il captatore sarebbe stato in grado anche di inviare una specifica notifica – notifica *push* – a ogni criptofonino, raggiungendo e copiando le chiavi di cifratura di ogni telefono in questione. Questo ulteriore passaggio è stato necessario in considerazione della modalità di criptazione utilizzata dalla piattaforma: *end to end*; la caratteristica di questa crittazione sta nell’individuazione in ogni dispositivo di una specifica chiave di crittazione e decrittazione, il che non permette – se non al titolare del dispositivo – di leggere il messaggio arrivato. Banalmente, in maniera analoga, è quello che accade con Whatsapp: il messaggio viene scritto dal mittente, al momento dell’invio il telefono lo cripta e lo recapita al destinatario che – grazie alla chiave di lettura presente nel dispositivo – lo decripta e lo rende leggibile, così che nessun altro possa decriptare e leggere il messaggio.

Così facendo, in sostanza, la Gendarmeria è stata in grado di decifrare sia i messaggi che fino a quel momento erano stati scambiati sulla piattaforma – ormai memorizzati – sia quelli che, in maniera dinamica, contestualmente, venivano mandati da un criptofonino e recapitati all’altro[1]

2 - Nel tentativo di comprendere le attività svolte...

Due sono le problematiche sorte dalla vicenda, l'una legata all'altra. La prima: come devono o possono essere qualificati gli atti di indagine svolti? E la seconda: gli Ordini europei di indagine emessi dall'autorità italiana sono validi?

Cominciando dalla prima domanda, occorre primariamente comprendere come si sia mossa l'autorità francese. A ben guardare, l'ordinanza emessa dal giudice d'oltralpe autorizzava l'istallazione del *trojan*, per poter procedere a un'attività captativa che aveva – quindi – portato all'acquisizione delle *chat* e di alcune chiavi di cifratura, oltre che alla captazione di messaggi dinamicamente scambiati dagli utilizzatori. Allo stesso modo, anche la seconda ordinanza – alla stregua della prima – aveva la funzione di permettere l'acquisizione immediata dei messaggi. In sostanza l'attività svolta dall'autorità francese se non esclusivamente attività di intercettazione era certamente un'attività di intercettazione combinata a un'acquisizione di documenti o dati informatici; un'attività che si potrebbe definire ibrida.

Infatti, nell'installare il *trojan*, di fatto, l'Autorità è stata in grado di svolgere sia un'attività di ricerca sia un'attività di sorveglianza così riuscendo ad acquisire tanto dati in tempo reale c.d. dati caldi quanto dati salvati nel sistema informatico, dati c.d. freddi.

Il problema non è tanto nella realizzazione delle predette azioni combinate, ma consiste, come diversa parte della dottrina ha già sostenuto[2], nell'inesistenza di una normativa in materia che specifichi e limiti le attività in questione o, meglio, le modalità con cui vengono svolte.

Considerando che i dati acquisiti dall'Autorità francese sono stati trasmessi in Italia per mezzo di un Ordine Europeo di Indagine, occorre chiedersi – necessariamente – in quali categorie individuate dal legislatore interno siano sussumibili le indagini svolte, quantomeno alcuni passaggi di quelle indagini che, come detto, appaiono ibride[3].

Cercando, appunto, di trovare un mezzo di ricerca della prova in cui incastonare questo tipo di attività, la perquisizione potrebbe essere una delle proposte: il *trojan*, infatti, è riuscito a penetrare nel *server* permettendo la lettura e la copiatura dell'*hard disk* e, dunque, l'intero contenuto del *server*. Questa sorta di ingresso, ricerca e acquisizione ha, però, evidenti differenze con la perquisizione "ordinaria": intanto queste intrusioni e relative apprensioni sono state occulte, cioè, senza la conoscenza del soggetto (*rectius*: dei

soggetti) che le subisce e senza che lo stesso possa rapidamente e chiaramente accorgersi dell'avvenuto accesso altrui e, poi, sono permanenti, perché di fatto – a differenza di un "banale" ingresso in abitazione (in caso di perquisizione locale), l'ottenimento dei dati richiede tempo. Infine, qualora si considerasse una perquisizione informatica quella svolta in Francia, quest'ultima – quantomeno per come realizzata nel caso in oggetto – ha permesso di visionare e di apprendere un'infinità di dati, non selezionati secondo criteri di ricerca per – a esempio – mittente, destinatario e contenuto. In sostanza, una volta entrati nel "luogo informatico" (*rectius*: spazio) non ci si è limitati a cercare quanto previsto dall'eventuale decreto di perquisizione, ma si è proceduto a tutto campo, come se si stesse utilizzando un "congegno bulimico"[4].

Tutto questo senza contare che con questi nuovi strumenti è possibile, come è stato fatto – nei casi in cui l'inoculazione del *trojan* non vada direttamente a buon fine – con un comportamento quasi "fraudolento", chiedere al proprietario dell'apparecchio tecnologico di effettuare delle operazioni che garantiscano all'operatore di attivare il *trojan,* quasi ottenendo un comportamento collaborativo del soggetto controllato, senza lasciare alcuna traccia[5]. Anche se la giurisprudenza, sul punto, non sembra riuscire a rinvenire un comportamento "truffaldino", visto che la Suprema Corte, investita dell'argomento, ha affermato che gli stratagemmi ora esemplificati non possono essere in alcun modo considerati strumenti in grado di incidere sulla liberà fisico morale dei soggetti passivi, non violando – quindi – l'art. 188 c.p.p.[6].

Ancora, l'attività svolta dall'Autorità in questione non appare neppure o per meglio dire, tantomeno, un'ispezione. Non è stata realizzata, infatti, una mera attività di visualizzazione e/o di descrizione di quanto visibile o percepibile circa persone, luoghi o cose; non si è operato con una mera osservazione del contenuto del *server,* ammesso che ciò sia possibile, anche perché nel caso in questione, trattandosi di messaggi criptati, una ispezione avrebbe permesso – al massimo – una lettura di chiavi e numeri che, certamente, non avrebbe permesso la comprensione del contenuto di quanto letto e, quindi, di quanto necessario ai fini delle indagini.

L'attività compiuta, anche se – magari – non nella sua interezza, sembra avvicinarsi di più – invero – una vera e propria intercettazione: un'infiltrazione in un sistema informatico che ha permesso l'apprensione occulta di conversazioni o comunicazioni in tempo reale da parte di soggetti terzi, estranei alla conversazione stessa[7]. Pur se non immediatamente compreso dai giudici italiani, forse anche per la portata delle indagini in questione, non si può dubitare della tipologia di attività svolta: è certamente vero che le Autorità hanno proceduto all'acquisizione anche di dati freddi con l'accesso al *server* e a tutti i dati in esso già contenuti, ma evidentemente la captazione di comunicazioni e messaggi in tempo reale vi è stata, anche solo – a quanto si comprende – per poter raggiungere le chiavi di cifratura necessarie per la lettura dei messaggi, visto che,

considerando il sistema di criptazione *end to end*, difficilmente la sola società Sky ECC avrebbe potuto fornire quanto utile alla decriptazione, fermo restando che la società non ha mai confermato di aver collaborato per fornire chiavi di cifratura o *password* e visto che molte di queste società fondano la loro costruzione proprio sulla *privacy* dei propri clienti e sull'impossibilità di trattenere e salvare dati in *server* a disposizione della società stessa o a rischio di intromissione di terzi.

Tra l'altro, anche rispetto al mezzo dell'intercettazione, che sembra essere il più confacente per l'investigazione in questione, una delle problematiche attiene alla modalità "a tappeto" con cui si è proceduto, considerando che – data la presenza di un primo procedimento "a monte", ma di diversi procedimenti "a valle" – l'Autorità non è stata in grado di individuare criteri di selezione specifici che identificassero alcuni telefoni o utenze, dovendo *hackerare* entrambi i *server* della società fornitrice, acquisendo tutto, quasi – appunto – "bulimicamente". Secondo il codice di rito, però, ciò non sarebbe possibile – almeno in Italia – visti i requisiti stringenti che limitano l'utilizzo del mezzo di ricerca in ragione della capacità invasiva che promana e che, nel caso di specie, ha manifestato[8].

Ora, non riuscire perfettamente a inquadrare l'attività svolta in uno dei mezzi di ricerca della prova presenti all'interno dell'ordinamento italiano potrebbe essere utile anche per – semplicemente – dire che si è proceduto con l'utilizzo di mezzi di ricerca atipici, che non trovano una normazione o compiuta regolamentazione nel nostro codice di rito[9].

Ma, a ben vedere, non è solo questo il punto: proprio in considerazione della difficoltà di catalogare il mezzo di ricerca della prova utilizzato, gli esiti di ciò a cosa corrisponderebbero? Quanto consegnato dalla Francia all'Italia, cos'è? Sono documenti informatici, è corrispondenza o sono esiti di intercettazioni e dalla risposta a questa domanda dipende anche la validità degli Ordini Europei di indagine emessi dall'Italia.

Ora, la Cassazione si è pronunciata a inizio novembre, con due sentenze "gemelle" [10] sostenendo che le attività francesi erano attività di captazione, quantomeno alcune, fermo restando che – in alcuni casi – possa essersi verificata una mera acquisizione di dati, ma la risposta non sembra univoca.

Se così fosse stato, le regole da seguire avrebbero dovuto essere quelle degli artt. 266 ss. c.p.p., eppure si è proceduto secondo l'art. 234 *bis* c.p.p. La dottrina, che si è già accinta a commentare la vicenda, ha fatto notare che le difficoltà si rinverrebbero proprio nel comprendere quale sia la fattispecie corretta da applicare e da utilizzare per l'emissione degli Ordini di indagine, prendendo in considerazione anche l'art. 254 c.p.p.

Cercando di fare chiarezza – per quanto possibile: l'art. 234 *bis* c.p.p. sarebbe applicabile – secondo un orientamento giurisprudenziale – anche nel caso in cui la messaggistica su *chat* (acquisita tramite O.E.I.), decriptata da altra attività, venga poi inviata al paese richiedente, considerando l'oggetto dell'O.E.I. come un dato freddo, documentale, conservato all'estero e non un flusso comunicativo[11]. Al contrario, secondo diverso orientamento, questo ragionamento sarebbe corretto solo nei casi di acquisizione di documenti e dati informatici c.d. dematerializzati e preesistenti rispetto all'avvio delle indagini o – comunque – formati fuori dalle investigazioni che poi li utilizzano.

Nel caso di specie sembra, piuttosto, che la documentazione acquisita sia in parte preesistente e in parte il risultato di un'attività di intercettazione dell'Autorità francese; alla luce di ciò, l'applicazione dell'art. 234 *bis* c.p.p. è discutibile, considerando che – appunto – quanto ottenuto dall'Autorità italiana si è concretizzato in un'apprensione occulta del contenuto del *server* della società fornitrice dei telefoni criptati e della relativa *app* di messaggistica, quindi, l'esito di un'intercettazione. Tra l'altro, per poter essere applicato – l'art. 234 *bis* c.p.p. – necessita del consenso del legittimo titolare, cioè o del mittente o del destinatario del messaggio; l'Autorità italiana ha sostenuto che il consenso sia stato legittimamente dato dall'Autorità francese, dato che il *trojan* inoculato aveva permesso di copiare i messaggi che pervenivano al *server* della società indagata anche a un *server* della stessa Autorità giudiziaria. Dunque, il legittimo titolare sarebbe stato – appunto – non la società proprietaria dell'*app* di messaggistica o mittenti e destinatari dei predetti messaggi, ma l'Autorità francese a seguito della copia effettuata. La motivazione fornita non è apparsa convincente, neanche alla Sesta Sezione nelle due sentenze del novembre 2023.

Un ulteriore problema sembra porsi in relazione all'art. 234 *bis* c.p.p.: la disposizione ammette che sia consentito acquisire dati e documenti informatici all'estero, senza bisogno di alcuna ulteriore autorizzazione se non il consenso del proprietario[12]. Allora, di fatto, quale sarebbe stato il motivo di emanazione di un O.E.I., quando, proprio la norma in questione garantisce una rapidità peculiare e un rapporto tra Autorità immediato?

È stata fatta notare la possibilità di applicare anche l'art. 254 *bis* c.p.p. concernente il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni[13]. Ciò sarebbe potuto avvenire se si fosse trattato di dati freddi, chiesti al fornitore che avrebbe garantito la realizzazione di una copia dei dati, ma – nuovamente – nel caso di specie sembra trattarsi di comunicazioni captate, di flussi, di dati dinamici. L'attività svolta, infatti, è stata occulta, nascosta alla società di messaggistica e, al contrario, il sequestro, pur essendo un atto a sorpresa, non avviene al di fuori della conoscenza del soggetto spossessato[14]. La società indagata, infatti, non ha mai sostenuto di aver consegnato quanto da lei

posseduto nei *server*, anche perché, di solito, queste piattaforme garantiscono ai propri clienti che nessun messaggio venga salvato o trattenuto negli archivi.

Volendo scendere ancora più in profondità, se fosse un mero sequestro di dati, sarebbe un sequestro ordinario o un sequestro di corrispondenza, dato che il fulcro della vicenda sono messaggi intercorsi tra diversi soggetti? Il problema, che si sovrappone a quello già considerato, sta nel concetto di corrispondenza. Quanto acquisito dall'Autorità italiana mediante O.E.I. è corrispondenza?

Il dubbio si è posto perché a una prima lettura sembrano rientrare tra i documenti di cui all'art. 234 o 234 *bis* c.p.p. i dati conservati in una memoria del telefono cellulare (e-mail, SMS e messaggi Whatsapp), mentre la corrispondenza e il relativo sequestro, sarebbero applicabili nel caso di un'attività di spedizione in corso.

Cercando di comprendere meglio i passaggi fondamentali, il rapporto tra intercettazione, acquisizione di documenti *ex* art. 234 c.p.p. e sequestro *ex* art. 253 c.p.p. sembra potersi individuare nel c.d. criterio dell'inoltro: l'invio del messaggio al destinatario e la captazione dinamica dello stesso genererebbe l'acquisizione di un flusso informatico, da sottoporre alla disciplina più specifica degli art. 266 ss. c.p.p. Al contrario, però, i messaggi Whatsapp e gli SMS presenti in un telefono cellulare non rientrano nel concetto di corrispondenza perché questa prevederebbe un'attività del mittente per la consegna o un'attività di spedizione a terzi[15].

In sostanza, se i messaggi – anche di posta elettronica – sono già stati ricevuti dal destinatario, pur non essendo dallo stesso ancora letti, si tratterà di un dato c.d. statico, per cui si può escludere l'applicazione della disciplina delle intercettazioni. Perciò, un conto è che l'Autorità proceda ad acquisire conversazioni in tempo reale, un conto sono le conversazioni già avvenute, la cui trasmissione si è già conclusa, per cui è possibile il sequestro.

In questo senso, quindi, le comunicazioni che hanno ormai raggiunto il recapito del destinatario, tenute nella memoria di un pc o di un telefono cellulare o, ancora, un *account* di gestione di posta elettronica dovrebbero rientrare nella disciplina del sequestro ordinario (*ex* art. 253 c.p.p.) e non nel sequestro di corrispondenza[16].

In realtà, rispetto al concetto di corrispondenza, non tutta la dottrina è concorde nell'escludere tale qualificazione a messaggi Whatsapp e SMS pur se già pervenuti al destinatario. Recente, infatti, è la

pronuncia della Corte Costituzionale[17] che ha completamente ribaltato l'orientamento precedente, riconoscendo le predette comunicazioni – contenute in un cellulare – tutelate *ex* art. 15 della Costituzione, anche se già ricevute dal destinatario, senza, quindi, quella distinzione tra attività di consegna e/o spedizione e "staticità" del dato ricevuto[18]. Rimane, dunque, corrispondenza – anche elettronica – quello scambio che ancora non ha perso quel "carattere di attualità in rapporto all'interesse alla sua riservatezza"[19].

Di fatto, quindi, per l'ordinamento interno quanto ricevuto dall'Italia per mezzo dell'O.E.I. dovrebbe essere considerata corrispondenza, con la conseguente applicazione della disciplina o degli artt. 266 ss. o dell'art. 254 c.p.p. o, come possibile, in caso di acquisizione sia di dati caldi sia di dati freddi, di entrambe le discipline.

Insomma, comprendere dove ci si trovi determina una differenza di disciplina di non poco conto.

Parlando di sequestro di documenti e, dunque, dell'acquisizione di notizie circa l'avvenuta comunicazione – in passato – tra due soggetti, è sufficiente un decreto del P.M., motivato, così come avviene per i tabulati telefonici, essendo sufficiente questa come tutela rispetto alla lesione della riservatezza generata. In questo senso, il decreto di sequestro, che deve contenere una motivazione circa la finalità che gli investigatori vogliono perseguire con il sequestro stesso, deve essere realizzato non violando il limite di quanto concretamente utile alle indagini, così da rispettare il principio di proporzionalità tra tutela e lesione del diritto del privato, evitando, dunque, le ipotesi di sequestri esplorativi, dichiarato illegittimo dalla stessa Corte di cassazione[20]. In realtà, comunque, occorre rilevare che non sono mancate pronunce che hanno escluso la lesione del principio in questione anche nei casi di sequestro dell'intero contenuto di un sistema informatico, a seguito delle necessità probatorie che si erano paventate[21]. Diversamente avviene quando si tratti di sequestro di corrispondenza, per cui l'art. 15 della Costituzione impone una riserva sia di legge sia di giurisdizione: in questo caso, quindi, considerando la recente lettura della Corte Costituzionale circa il concetto di corrispondenza, i messaggi e le *chat* sequestrate ricadrebbero – di diritto – nell'art. 254 c.p.p. piuttosto che nell'art. 253 c.p.p. Dunque, l'Autorità interna non avrebbe potuto operare senza quantomeno prima chiedere l'autorizzazione al giudice competente. Analogamente, in caso di intercettazioni, considerata la maggiore incisività nella sfera privata dell'individuo, non è sufficiente un decreto dell'organo di accusa. Infatti, anche questa disciplina è sottoposta a una riserva sia di legge sia di giurisdizione: non solo le intercettazioni possono essere effettuate solo nei casi e nei modi previsti da legge, ma è un giudice – di solito il G.I.P. – ad autorizzarle con un decreto motivato. Seppure il P.M. dovesse procedere con urgenza disponendo direttamente le intercettazioni, la comunicazione al giudice competente deve garantire l'emanazione di un decreto, da parte di quest'ultimo, nelle successive quarantotto ore. In caso di mancata

convalida si assisterebbe all'immediata interruzione dell'attività e all'inutilizzabilità dei dati raccolti.

Saper distinguere quando l'attività svolta sia stata un'intercettazione o un sequestro di documenti (seppure più nello specifico di corrispondenza) permetterebbe agli interpreti di chiedersi e di comprendere se i risultati delle intercettazioni siano utilizzabili nell'ordinamento interno e se fosse servito un controllo preventivo o successivo sui dati[22].

Ebbene, volendo fare un passaggio ulteriore, come si poteva immaginare, l'attività – captativa o meno che sia – ha coinvolto diversi soggetti che ora sono indagati in Italia, alcuni di questi anche sottoposti a misure cautelari. La qualificazione dell'attività investigativa come attività di intercettazione determinerebbe la possibilità o necessità di applicare l'art. 270 c.p.p. per far sì che in tutti i procedimenti interni, concernenti la vicenda, possano essere utilizzate le relative intercettazioni. La questione sorge perché il fatto, nel suo complesso, è piuttosto articolato: da un primo procedimento "a monte" – francese – nel quale sono state autorizzate le intercettazioni, vista la portata transfrontaliera dell'indagine, sono scaturiti diversi procedimenti nazionali a carico di singoli indagati, nei confronti dei quali sono state anche applicate misure cautelari, proprio alla luce di quanto emerso dagli esiti delle intercettazioni. Il problema dell'utilizzabilità nell'ordinamento, infatti, sembra legata alla capacità di utilizzo degli stessi esiti nei singoli procedimenti. Il punto, in effetti, è che la regola generale di cui si legge nel primo comma dell'art. 270 c.p.p., afferma l'inutilizzabilità dei risultati delle intercettazioni in procedimenti diversi da quelli per cui sono state disposte, ma è immediatamente derogabile, così come previsto dalla seconda parte del medesimo comma, in caso di rilevanza e indispensabilità per l'accertamento. L'eccezione cui ci si riferisce appare piuttosto ampia, discrezionalmente orientata e tale da permettere di "annullare" la regola[23]. A ciò è necessario aggiungere che il comma 1 *bis* del medesimo articolo afferma che le intercettazioni tra presenti realizzate con un captatore informatico installato su un dispositivo elettronico possono essere utilizzati anche per la prova di reati diversi da quelli per cui il decreto è stato emesso[24].

Non è un caso, infatti, che la Corte di cassazione[25] abbia nuovamente adito alle Sezioni Unite, per comprendere – appunto – se i risultati delle intercettazioni, ottenute mediante l'ordine europeo di indagine, integri quanto previsto dall'art. 270 c.p.p. Si ripropone, quindi, un problema che già con la Riforma del 2020 in tema di intercettazioni si era compreso: il significato dei termini rilevanza e indispensabilità e di diverso procedimento. A ben vedere, infatti, la dicotomia non solo non sembra esprimere una vera e propria capacità selettiva o discretiva dei procedimenti diversi nei quali i risultati delle intercettazioni possono essere utilizzati, ma si riduce al concetto di indispensabilità, perché – di fatto – il concetto di rilevanza è in gioco anche con riguardo ai reati connessi e non solo a quelli diversi, ulteriori[26]. Per quanto concerne il diverso

procedimento la Suprema Corte[27] si era già pronunciata sostenendo che il divieto non opera per i procedimenti connessi secondo l'art. 12 lett. a) c.p.p. a quelli per i quali all'inizio l'intercettazione era stata disposta. Alla luce anche dei contrastanti orientamenti giurisprudenziali, sempre con la Riforma del 2020, il legislatore, modificando l'art. 270 c.p.p., ha deciso di normare che l'utilizzo nei diversi procedimenti è possibile (oltre che nel caso di indispensabilità e rilevanza) nei casi in cui si accertano i reati di cui all'art. 266 c.p.p.[28]. Numerose le interpretazioni di diverso procedimento realizzate dalla dottrina; per ciò che qui interessa, il dubbio viene se si pensa che il concetto di procedimento diverso non coincide con l'eventuale frazionamento di un procedimento all'origine unitario, ma che necessita – appunto – di una scissione per l'eterogeneità delle ipotesi di reato o per il numero di indagati. La diversità deve consistere proprio in relazione al fatto e non coinvolge neanche la possibilità che emergano, nell'ambito di un unico e principale procedimento, diversi reati; insomma, si deve trattare di un procedimento diverso inteso in senso sostanziale[29].

Alla luce di ciò: i procedimenti "a valle" dell'indagine principale transnazionale sono o no procedimenti diversi che necessiterebbero dei risultati delle intercettazioni per indispensabilità o perché, comunque, rientranti negli artt. 266 ss.?

3 - ...Un rapido sguardo al contenuto degli Ordini europei di indagine

Secondo quanto è stato detto rispetto all'attività svolta che, si ripete, secondo alcune sentenze della Suprema Corte sarebbe, quantomeno in parte captativa, l'autorità giudiziaria italiana cosa avrebbe dovuto fare? Emanare un O.E.I. per delle intercettazioni o avrebbe dovuto, come ha fatto, semplicemente chiedere all'autorità francese di decriptare le conversazioni dalla stessa – forse autonomamente e senza previa richiesta – acquisite e poi inviarle, avendo – quindi – in mano semplicemente dei documenti?

Senza volersi dilungare, l'Ordine Europeo di Indagine consiste in una decisione giudiziaria che viene emessa da un paese europeo al fine di ottenere atti di indagine effettuati in un altro paese; dunque, la direttiva che lo ha costruito[30] aveva la finalità di creare un sistema globale di acquisizione di prove in tutte quelle fattispecie di reato in grado di avere una dimensione transfrontaliera. Il fondamento dello strumento in questione è individuabile nell'art. 82 TFUE concernente la cooperazione giudiziaria nell'Unione europea e, in particolare, sul principio del mutuo riconoscimento. Quest'ultimo, oggi oggetto di un titolo apposito nel codice di rito, è stato introdotto nel 2017 per garantire la cooperazione tra gli Stati in una sorta di "regime di fiducia reciproca". Di fatto, quindi, alla richiesta proveniente da uno Stato viene data attuazione in un diverso

Stato, senza che – però – ci siano duplici controlli di legittimità e senza un potere di sindacabilità sull'attività l'uno dell'altro. Infatti, l'autorità di emissione dell'ordine non ha il potere di sindacare, appunto, le misure adottate dallo Stato di esecuzione per raccogliere le prove; per cui, spetta allo stato Stato di esecuzione conoscere le corrette modalità di acquisizione e a quello di emissione verificare se l'ordine sia legittimamente emesso, oltre che l'utilizzabilità nel procedimento interno di quanto acquisito[31]. Ciò significa che ogni Autorità collabora, ciascuna con i propri strumenti giuridici e sulla base, però, di atti emessi da altri Stati in ragione del rispettivo diritto.

Le condizioni per l'emissione dell'O.E.I. sono il rispetto dei principi di equivalenza e proporzionalità, come stabilito dall'art. 6 della Direttiva[32]; proprio in relazione a questi principi, infatti, l'atto di indagine oggetto dell'O.E.I. deve essere compiuto nel rispetto delle stesse condizioni che si sarebbero attuate se fosse stato realizzato nello stato richiedente o, come specificamente dice la direttiva "alle stesse condizioni in un caso analogo". Ciò per evitare, secondo parte della dottrina, che l'Autorità giudiziaria possa aggirare le regole di acquisizione probatoria interna chiedendo ad altre Autorità di procedere – appunto – attraverso diverse modalità[33]. Nel caso dello stato italiano, sarebbero utilizzabili, alla luce di quanto previsto dall'art. 191 c.p.p., i materiali uscenti dal procedimento francese solo in caso di rispetto delle norme inderogabili interne, tra cui – le più importanti – il diritto al contraddittorio sulla prova e per la prova (di cui all'art. 111 co. 2 e 4 Cost.), il principio di legalità processuale (di cui al comma 1 dell'art. 111 della Costituzione), il diritto di difesa (*ex* art. 24 della Costituzione) e della liberà morale, di cui all'art. 188 c.p.p.[34].

Ancora, l'O.E.I. è attivabile solo quando proporzionato e necessario per il procedimento penale interno allo Stato richiedente, anche questo per evitare che singole Autorità giudiziarie possano abusarne quando gli stessi atti non sarebbero giustificati nell'ordinamento interno per la tipologia di procedimento, entità della pena eventualmente da irrogare e rilevanza dei fatti[35]. Il principio di proporzionalità impone che l'attività compiuta sia funzionale e adeguata in relazione al presupposto, cioè al fatto che si deve perseguire e alle conseguenze, cioè all'obiettivo che l'ordinamento vuole perseguire, considerando che si dovrebbe sempre realizzare l'attività meno lesiva dei diritti e delle libertà dell'indagato o imputato. È, però, proprio in relazione a questo art. 6 della Direttiva che potrebbero sorgere questioni; il controllo di proporzionalità appare centrale nella dialettica tra i due Stati, ma occorre comprendere se – oltre all'autorità emittente – anche quella ricevente possa operare una valutazione in merito, verificando che non ci siano soluzioni diverse, alternative e meno lesive di diritti fondamentali dei privati[36]. La Direttiva sembra affidare in maniera esclusiva all'autorità che emette il provvedimento l'interpretazione del proprio diritto secondo il quale sarebbe realizzabile un atto di indagine e trasferibile il risultato dell'attività investigativa; solo il rispetto di tutte le condizioni richieste dall'ordinamento interno per l'acquisizione e la circolazione delle prove richieste

permetterebbe l'emanazione di un O.E.I. Questo requisito, infatti, sembra poterlo accertare solo l'Autorità che emette l'ordine e difficilmente anche quella che è chiamata a eseguirlo, anche perché il riconoscimento di poteri per il vaglio di proporzionalità dell'O.E.I. in capo all'Autorità di esecuzione comporterebbe una deroga al principio del mutuo riconoscimento, seppur in un'ottica di tutela dei diritti dei privati colpiti dall'atto investigativo (c.d. principio di autonomia procedurale). Concretamente, il principio opera per garantire che lo Stato che emette l'ordine possa avere assicurato – a livello europeo – che l'atto da esso realizzabile all'interno dell'ordinamento sia effettuabile anche a livello europeo. In maniera analoga, infatti, l'Autorità che procede all'esecuzione dell'atto investigativo, lo farà seguendo le regole procedurali interne, senza che l'Autorità di emissione dell'O.E.I. possa sindacarne la modalità di svolgimento.

Si tratta, in sostanza, di due poteri esclusivi, in capo a due differenti Autorità e che, però, devono riconoscersi proprio in ragione del mutuo riconoscimento. Ciò chiaramente potrebbe comportare alcune problematiche di attuazione, soprattutto quando la normativa interna dei diversi Stati è completamente differente, a esempio, nel caso in cui la modalità di acquisizione di una prova non sia legittima nello stato richiedente, bensì legittima in quello di esecuzione. Anche perché non sarebbe coerente ammettere che lo Stato di esecuzione possa rifiutarsi di eseguire quanto richiesto in considerazione dell'eventuale illiceità o inutilizzabilità dell'acquisizione probatoria per il diritto interno dello Stato di emissione. La Direttiva riconosce un'unica possibilità di rifiuto da parte dello Stato di esecuzione, armonizzando il limite all'esecuzione e individuandolo nell'art. 6 della Carta di Nizza e dei diritti fondamentali dell'Unione Europea[37].

4 - Precarie conclusioni

Premesso che le conclusioni possono essere solo precarie vista la materia *in divenire*, secondo quanto detto fino a ora, l'utilizzabilità dell'esito dell'attività francese dipende dalla possibilità, da parte dell'Autorità italiana, di svolgere la medesima attività nel paese. Ammettendo che l'indagine svolta fosse un'intercettazione occorre chiedersi se fosse stato possibile realizzarla in Italia da parte degli investigatori considerati i limiti dettati dagli artt. 266 ss. c.p.p. in ragione dell'incisività del mezzo di ricerca della prova in questione. Una risposta negativa comporterebbe, da un lato, la liceità della richiesta e la legittimità dell'operazione in Francia, ma, dall'altro lato, l'inutilizzabilità dell'esito delle intercettazioni in Italia. Inutilizzabilità che potrebbe dipendere, tra l'altro, anche dall'assenza di una espressa autorizzazione da parte del G.I.P. competente; come detto, infatti, a differenza di altri mezzi di ricerca della prova, per le intercettazioni non può mancare il decreto motivato del giudice che autorizza l'attività stessa. Nel caso di specie, seppure non nell'O.E.I., visto

che questo è emesso direttamente dalle Procure, queste ultime si sarebbero dovute premunire di un decreto dell'Autorità giudiziaria per potersi garantire una corretta acquisizione della prova secondo il diritto interno[38].

In maniera analoga, nel caso in cui l'attività svolta fosse stata una copia del dato informatico contenuto nel *server,* per poter essere utilizzata bisognerebbe accertare il rispetto delle regole concernenti la copia forense a tutela della genuinità del dato informatico[39].

Non a caso, infatti, la questione è stata rimessa alle Sezioni Unite dalla Terza sezione penale[40] al fine di comprendere: la corretta modalità di acquisizione dei messaggi intercorsi nelle *chat* criptate in termini di documenti e/o dati informatici, *ex* art. 234 bis c.p.p.; la necessità di una verifica o autorizzazione da parte dell'Autorità giurisdizionale italiana.

Ancora, proprio sulle questioni ora sollevate, le Sezioni Unite saranno anche chiamate – questa volta investite dalla Sesta Sezione – ad approfondire due ulteriori sfaccettature problematiche: se l'acquisizione mediante O.E.I. dei risultati delle intercettazioni integri quanto previsto dall'art. 270 c.p.p. e se occorresse o meno un controllo preventivo o successivo dell'Autorità giurisdizionale italiana in ordine alla utilizzabilità dei dati raccolti[41].

Il quadro interno è piuttosto lacunoso sia perché manca nell'ordinamento interno una disciplina in grado di normare anche le nuove tecnologie e la conseguente nascita di nuovi mezzi di ricerca e acquisizione di dati virtuali sia – forse – per la scelta a monte operata nella Direttiva. Non si sono uniformate le norme processuali penali interne, considerando che ogni Stato continua a operare seguendo le proprie procedure, ma si sono uniformati i limiti che l'attività transfrontaliera non può superare; di fatto, la garanzia è che nello stato di emissione vengano rispettati diritto di difesa e il principio del giusto processo. Dunque, anche qualora l'attività investigativa fosse legittimamente svolta nel paese di esecuzione, secondo la *lex loci*, quanto assunto potrebbe non essere utilizzato dal paese di emissione se l'attività dovesse risultare in contrasto con i principi dell'ordinamento interno, secondo la *lex fori**[42]*.

Un ulteriore problema di inutilizzabilità – non irrilevante – si è posto e attiene al principio del contraddittorio; quest'ultimo – quale principio interno fondamentale – deve essere necessariamente rispettato per far sì che le prove acquisite all'estero possano trovare posto in Italia[43]. Chiaramente, la rilevanza del contraddittorio concerne la possibilità di esercitare una difesa adeguata, in relazione alla presunzione di non colpevolezza

nell'arco di tutto il processo e alla formazione della prova in condizione di parità tra le parti, per una tutela del corretto accertamento giurisdizionale[44]. Difatti, l'art. 111 co. 2 Cost., considerata la natura precettiva della norma e, dunque, immediatamente applicabile al processo penale, dispone che vi sia l'obbligo di garantire la piena partecipazione all'attività istruttoria, nella sua interezza, in aderenza anche con quanto previsto dall'art. 6 C.E.D.U.[45] Sul punto la giurisprudenza si è espressa, non sempre in maniera uniforme, per le vicende di messaggistica mediante Blackberry, per cui – secondo un orientamento – anche quando l'attività di intercettazione è legittimamente compiuta, è necessario assicurare che la decriptazione dei messaggi avvenga o alla presenza dei difensori o – quantomeno – è doveroso che la difesa possa ottenere la versione criptata dei messaggi e le relative chiavi di decriptazione, pena la nullità di ordine generale e a regime intermedio di cui all'art. 178 lett. c) c.p.p.[46]. Al contrario, secondo un diverso orientamento, l'attività di messa in chiaro dei messaggi non potrebbe comportare alcun errore o interferenza da parte degli investigatori o delle procure, perché – proprio la stretta relazione con la scienza informativa – permetterebbe di ottenere solo risultati fedeli anche nella riproduzione. Quindi, la mancata disponibilità per la difesa dei *files* originari non è lesiva del diritto di cui all'art. 24 della Costituzione considerando anche che non si tratterebbe di un problema di legittimità o utilizzabilità, bensì di affidabilità del dato[47]. Dunque, l'ordinamento interno garantirebbe solo la certezza della c.d. catena di custodia per tutelare l'integrità probatoria, ma non anche l'accesso agli algoritmi da parte della difesa.

Seguendo il secondo orientamento, bisognerebbe, a prescindere dall'attività svolta in Francia, acquisizione di dati freddi o caldi, per quanto concerne la successiva attività di decriptazione non presumere, che quanto decriptato corrispondesse perfettamente al messaggio criptato, senza margini di errore o alterazione[48]. Anche non volendo avere retropensieri, è comunque vero che l'attività di decriptazione richiede lo svolgimento di azioni tecniche e specialistiche, sicuramente non effettuate dall'Autorità giudiziaria, ma da terzi, seppure da essa nominati e in questo lavoro potrebbero realizzarsi condizionamenti alle prove che non sarebbero mai verificabili o controllabili, né dal giudice italiano né dal difensore[49].

Insomma, considerati i dubbi che emergono dal caso in questione, quale mezzo di ricerca della prova è stato utilizzato, ammesso che ce ne sia uno tipico? Quale doveva essere inserito all'interno dell'Ordine Europeo di Indagine? Quali margini di utilizzabilità ci sono nei singoli procedimenti interni, anche cautelari?

Non ci resta che aspettare le due pronunce delle Sezioni Unite.

[1] M. T. Morcella, *Le due mosse, con cui l'AG francese ha "hackerato" Sky ECC*, in *Dir. pen. proc*., 2023, 10, *passim*. Per ulteriori approfondimenti e spiegazioni tecniche, D. Curtotti, V. Rizzi, W. Nocerino, A. Russitto, G. Gilberti, G. Scarpa, *Piattaforma criptata e prova penale*, in *Sist. pen*., 2023, 6, *passim*; sul tema anche N. Gallo, *Un tassello giurisprudenziale in tema di Ordine Europeo di Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, in *Arch. pen*. (web), 2023, 3, *passim*.

[2] Tra gli altri, G. Spangher, *Chat. Saranno le Sezioni Unite a "decriptare" le questioni giuridiche*, in *www.giustiziainsieme.it*, 13 novembre 2023.

[3] Sul tema, tra gli altri, W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*, in *www.penaledp.it*, 29 novembre 2023.

[4] O. Dodero, *Intercettazioni: il trojan e l'utilizzabilità (parte terza)*, in *www.unicost.eu*, 18 maggio 2020.

[5] L. Filippi, *Il cavallo di Troia e l'ispe-perqui-intercettazione*, in *www.penaledp.it*, 21 marzo 2022.

[6] C. Cass., Sez. V, 30 settembre 2020, n. 31064.

[7] C. Cass., S.U., 24 settembre 2003, n. 36747.

[8] Sul punto, C. Cass., Sez. VI, 9 dicembre 2020, dep. 2021, n. 6623, Pessotto, in *Mass. Uff.*, n. 280838-01.

[9] Tra gli altri, in considerazione della specificità dell'argomento e sottili differenze, L. Ludovici*, I criptofonini: sistemi informatici criptati e server occulti*, in *www.penaledp.it*, 14 ottobre 2023; F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. De Direito Processual Penal*, vol. 3, 2, 489. Considerando anche che la perquisizione online può essere disposta direttamente dal P.M., senza l'autorizzazione del G.I.P.; in questo senso C. Cass., Sez. V, 14 ottobre 2009, Virruso, in *Mass. Uff*., n. 246954.

[10] C. Cass., Sez. VI, 2 novembre 2023, n. 44154; Id., Sez. VI, 2 novembre 2023, 44155.

[11] C. Cass., Sez. IV, 5 aprile 2023, n. 16347, Papalia, in *Mass. Uff*., n. 284563; Id., Sez. I, 13 gennaio 2023, n. 19082, Costacurta, in *Mass. Uff*., n. 284440; Id., Sez. I, 13 ottobre 2022, dep. 2023, n. 6364, in *Mass. Uff*., n. 283998; Id., Sez. VI, 20 aprile 2021, n. 18907, in *Mass. Uff*., n. 281819.

[12] In giurisprudenza, C. Cass., Sez. VI, 27 settembre 2023, n. 46482, Bruzzaniti, in *Mass. Uff*., n. 285363-03.

[13] C. Cass., Sez. VI, 26 ottobre 2023, Kolgjokaj.

[14] L. Filippi, *Il cavallo di Troia e l'ispe-perqui-intercettazione*, cit.

[15] C. Fontani, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Dir. pen. proc*., 10, 2023, 1313 s.; M. Torre, *WhatsApp e l'acquisizione processuale della messaggistica istantanea*, in *Dir. pen. proc*., 2020, 9, 1281; C. Cass., 22 agosto 2022, n. 31364 in cui la Suprema Corte ha ribadito che i messaggi whatsapp come gli SMS conservati nel cellulare hanno rilevanza *ex* art. 234 c.p.p., dunque, l'acquisizione non soggiace né alle regole sulla corrispondenza, né a quelle delle intercettazioni; Id., Sez. V, 21 novembre 2017, n. 1822; Id., Sez. III, 25 novembre 2015, Giorgi, in *Mass. Uff*., n. 265991.

[16] A. Vele, *Documento informatico e tutela della riservatezza nel processo penale: aspetti problematici*, in *Arch. Pen*. (web), 2018, 1, 7 s.; C. Cass., Sez. I, 1° luglio 2022, n. 34059; Id., Sez. III, 16 aprile 2019, n. 29426.

[17] C. Cost., sent. 170 del 2023.

[18] G. Spangher, *Servono regole di garanzia per la prova informatica*, in www.penaledp.it, 12 ottobre 2023.

[19] C. Cost., sent. 170 del 2023.

[20] Sull'illegittimità del sequestro avente fini esplorativi, Cass., Sez. VI, 30 ottobre 2020, in *Giur. pen*., 3 novembre 2020.

[21] C. Cass., Sez. un., 19 aprile 2018, n. 36072; Id., Sez. un, 20 luglio 2017, n. 40963; in dottrina, W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*, cit.

[22] Domanda che si è posta la Sesta Sezione della Corte di cassazione che con la sentenza 15 del 2021 ha rimesso il quesito alle Sezioni unite.

[23] E.N. La Rocca, *L'art. 270 c.p.p. e la proporzionalità perduta: moniti per un recupero dalla Corte di giustizia UE*, in *Arch. pen*., 2021, 1, 137.

[24] Sul tema, nello specifico, E.N. La Rocca, *L'art. 270 c.p.p. e la proporzionalità perduta: moniti per un recupero dalla Corte di giustizia UE,* cit., 141 ss.

[25] C. Cass., Sez. VI, 15 gennaio 2024, 1.

[26] F. Alvino, *La circolazione delle intercettazioni e la riformulazione dell'art. 279 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, in *Sist. pen*., 2020, 5, 242.

[27] C. Cass., Sez. un., 2 gennaio 2020, n. 51, in *Sist. pen*., con nota di G. Illuminati, *Utilizzazione delle intercettazioni in procedimenti diversi: le Sezioni Unite ristabiliscono la legalità costituzionale*, 30 gennaio 2020.

[28] Sul tema, D. Albanese, *Sull'utilizzabilità dei risultati delle intercettazioni nell'ambito del "medesimo procedimento": il Tribunale di Milano prende le distanze dalle Sezioni unite "Cavallo",* in *Sist. pen*., 1° dicembre 2020; S. Chelo, *Divieto di utilizzabilità delle intercettazioni telefoniche in procedimenti diversi: le Sezioni Unite scelgono la via garantista*, in *Proc. pen. giust*., 2020, 4, *passim*.

[29] Sul punto, di recente, dato il nuovo contrasto giurisprudenziale, M. Griffo, *Non c'è pace per l'articolo 270 c.p.p.: un recente contrasto in ordine ai presupposti di applicabilità della "nuova" disciplina*, in *Arch. pen.* (web), 2023, 2, *passim*.

[30] D. 2014/41/UE.

[31] A. Gaito, *Spazio penale europeo e cooperazione giudiziaria internazionale*, in A.A. V.V., *Procedura penale*, Torino, 2019, VII, 975 s. Di recente, in giurisprudenza, C. Cass., Sez. VI, 26 ottobre 2023, n. 46833, Bruzzaniti, non massimata.

[32] Sul tema, R.E. Kostoris, La tutela dei diritti fondamentali, in Manuale di procedura penale europea, Milano, 2017, III ed., 90 ss.

[33] Sul punto si è pronunciata la Corte di Lussemburgo, 16 dicembre 2021, C-724/2019.

[34] L. Filippi, *Criptofonini e diritto di difesa*, in *www.penaledp.it*, 23 giugno 2023.

[35] M. Caianelo, La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove, in Proc. pen. giust., 2015, 3, 5-6.

[36] Sul punto M. Daniele, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa dele Sezioni Unite*, in *Sist. pen.* (web), 11 dicembre 2023.

[37] Le questioni sono state sollevate dal prof. E. Cannizzaro durante il Convegno tenutosi presso l'Unitelma Sapienza durante il Convegno Criptofonini, in attesa delle Sezioni Unite, tenutosi il 6 dicembre 2023.

[38] F. Resta, *Criptofonini e ordine europeo di indagine: le questioni poste alle Sezioni Unite*, in *www.giustiziainsieme.it*, 16 novembre 2023.

[39] A. Barbieri, *I limiti all'utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*, in *www.giurisprudenzapenale.it*, 6 febbraio 2023, *passim*.

[40] La rimessione è avvenuta con la decisione n. 9 del 2023 da parte della Terza sezione penale della Corte di cassazione.

[41] C. Cass., Sez. VI, 15 gennaio 2024 per i singoli motivi di rimessione; per la motivazione C. Cass., Sez. VI, 15 gennaio 2024, n. 2329, in *www.penaledp.it*, 16 gennaio 2024.

[42] C. Cass., Sez. VI, 2 novembre 2023, n. 44154

[43] Sul punto Cass., Sez. IV, 7 settembre 2022, n. 32915.

[44] F.R. Dinacci, *L'inutilizzabilità nel processo penale*, Milano, 2008, 4.

[45] A. Barbieri, *I limiti all'utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine,* cit., 10.

[46] A. Barbieri, *I limiti all'utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine,* cit.; L. Filippi, *Quattro miti da sfatare sull'intercettazione dei cellulari blackberry,* in www.penaledp.it, 28 febbraio 2023; G. Pittelli, F. Costarella, *Ancora in tema di chat "pin to pin" su sistema telefonico BackBerry*, in *Arch. pen*. (web), 2016, 1, passim. Sul tema in giurisprudenza, Cass., Sez. IV, 15 ottobre 2019, Brandimarte, n. 49896, in *Mass. Uff*., 277949-01; Id., Sez. IV, 15 luglio 2022, n. 32915, Lori, non massimata.

[47] C. Cass., Sez. III, 21 aprile 2022, n. 30395, Chiancano, in *Mass. Uff*., n. 283454-01; Id., Sez. III, 10 maggio 2019, n. 38009, Assisi, in *Mass. Uff*., n. 278166-02.

[48] C. Cass., Sez. I, 13 ottobre 2022, dep. 2023, Calderon, in *Mass. Uff*., 283998; Id., Sez. I, 13 ottobre 2022, dep. 2023, Minichino, non massimata.

[49] La dottrina ha dibattuto sulla possibilità di ricondurre al vizio della nullità o dell'inutilizzabilità la mancata partecipazione dell'imputato alla formazione della prova; di fatto, se da un lato la violazione del principio del contraddittorio nella formazione della prova non consiste in una violazione del diritto di difesa inteso nel senso di cui all'art. 178 c.p.p., dunque, come diritto di partecipazione e assistenza tecnica, dall'altra garantisce una tutela maggiore. Appare più corretto, però, continuare a riferirla al vizio dell'inutilizzabilità, dato che sembra concernere la formazione della prova in sé considerato. Sul punto, Barbieri, *I limiti all'utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine,* cit., 12.