# I criptofonini e le garanzie perdute.

*Cryptophones and lost guarantees*

Luigi Ludovici
Associato di Diritto processuale penale nell'Università degli Studi "Guglielmo Marconi"

Sommario: 1. La captazione della messaggistica criptata nel quadro generale del sistema 2. I *criptofonini*: il problema delle intercettazioni *omnibus* 3. *Segue*: acquisizione dell'algoritmo e violazione del domicilio digitale 4. *Segue*: stringhe informatiche, chiavi di cifratura e diritto al contraddittorio 'per la prova'

**ABSTRACT**

La giurisprudenza della Corte di cassazione ha fatto registrare, negli ultimi anni, la comparsa di un serrato contrasto sulla utilizzabilità nei procedimenti penali italiani del materiale probatorio acquisito all'estero mediante la captazione e la decrittazione dei flussi comunicativi scambiati dagli utenti attraverso l'impiego dei c.d. criptofonini. L'Autore, a commento del duplice e coevo intervento reso di recente dalle Sezioni Unite, si sofferma sui principali profili problematici che innervano la tematica, mettendo in luce le tensioni che talune soluzioni offerte dal plenum generano con i principi del giusto processo.

*In recent years, the jurisprudence of the Court of Cassation has led to the emergence of a sharp contrast on the usability in Italian criminal proceedings of evidentiary material acquired abroad through the capture and decryption of communication flows exchanged by users through the use of so-called cryptophones. The Author, commenting on the double and contemporary intervention recently made by the United Sections, dwells on the main problematic profiles that innervate the issue, highlighting the tensions that some solutions offered by the plenum generate with the principles of due process.*

## 1. La captazione della messaggistica criptata nel quadro generale del sistema

Con la diffusione sempre più massiva di applicazioni e programmi capaci di inviare e ricevere in tempo reale testi scritti ma anche *file* audio e video, pdf, fotografie, il monitoraggio e l'acquisizione dei flussi comunicativi così veicolati rappresentano oggi, senza tema di smentita, tra le attività che maggiormente impegnano gli organi investigativi, e questo non soltanto in Italia ma anche all'estero.

Naturalmente, si tratta di forme di comunicazione che, in quanto tali, godono della copertura costituzionale offerta dall'art. 15 Cost. e che quindi

possono essere limitate soltanto per atto motivato dell'autorità giudiziaria, con le garanzie stabilite dalla legge.

Sappiamo che la declinazione del principio costituzionale a livello di legislazione ordinaria assume connotati assai più rigorosi, allorquando l'atto investigativo riguardi flussi comunicativi in corso di svolgimento, e si estrinsechi sotto forma di monitoraggio occulto condotto da un soggetto estraneo alla comunicazione stessa: al ricorrere di tali condizioni ci troviamo, come è noto, in presenza di una intercettazione[1], con conseguente applicazione del rigoroso regime delineato dagli artt. 266 ss. c.p.p.

Ebbene il discorso non muta quando oggetto dell'azione investigativa è la messaggistica istantanea: è pacifico, infatti, che quando questa forma di comunicazione venga interessata da una attività captativa occulta, la disciplina applicabile è quella delle intercettazioni telematiche ex art. 266-bis c.p.p. Ne segue che l'atto intrusivo potrà trovare luogo, anche in questo caso, solamente previa autorizzazione dell'organo giurisdizionale, al ricorrere dei presupposti oggettivi, funzionali e probatori prescritti dalla legge.

Occorre peraltro sottolineare che questa ricostruzione non ha trovato occasioni di smentita neppure nel quadro dei principi affermati dalla Consulta nella nota sentenza n. 170 del 2023. Superando la concezione tradizionale, la Corte costituzionale[2] ha, infatti, chiarito che il discrimine tra ciò che costituisce corrispondenza e ciò che invece non lo è più è rappresentato non da se la comunicazione sia o meno in transito dal mittente al destinatario, ma dalla persistenza, nei soggetti coinvolti, di un interesse attuale alla riservatezza della comunicazione tra loro intercorsa.

Ora, senza voler entrare nel merito delle conclusioni raggiunte dalla Corte costituzionale, quello che è certo è che l'inedita - e forse ipertrofica - concezione di "corrispondenza" così propugnata non genera affatto frizioni con il diverso principio secondo cui la captazione occulta di testi inviati via *chat* o a mezzo di posta elettronica, se realizzata senza ostacolarne il contestuale svolgimento, continua di per sé ad integrare una attività di tipo intercettivo: questo perché il sequestro della messaggistica, sia che interrompa il flusso comunicativo (art. 254) sia che intervenga a valle del suo compiersi (art. 253), è un atto che implica sempre l'ablazione della *res*, cioè del supporto fisico nel quale il pensiero è incorporato, mentre l'intercettazione attinge direttamente (ed esclusivamente) al suo contenuto, memorizzandolo: che è proprio quello che accade quando si monitorano in tempo reale i messaggi inviati all'interno di una chat individuale

[1] La nozione di intercettazione riportata nel testo, da tempo affermatasi in seno alla giurisprudenza di legittimità, (cfr., *ex multis*, Sez. Un., 28/05/2003, Torcasio, in C.E.D. Cass., n. 225465-01), è stata recentemente ribadita anche dalla Consulta nella nota sentenza sul c.d. caso Renzi (C. cost. sent. n. 170 del 2023, in *www.discrimen.it*, 26 ottobre 2023, con nota di R. ORLANDI, *"Corrispondenza" dei Parlamentari e limiti all'accertamento penale nella sentenza n. 170 del 2023 della Corte costituzionale*.

[2] C. cost., sent. n. 170 del 2023, cit.

o di gruppo grazie, ad esempio, ad un malware che sia stata inoculato nel dispositivo portatile del soggetto impegnato nella comunicazione.

Ma se dunque l'inquadramento, sotto il profilo giuridico, del tipo di attività necessaria per la captazione delle *chat* non desta di per sé particolari problemi, sappiamo che un primo elemento di complessità discende dal fatto che questi servizi di comunicazione istantanea sono, di regola, dotati di sistemi di crittografia tali da rendere inintellegile dall'esterno il contenuto delle comunicazioni intercorse tra gli utenti abbonati.

Così, per il buon esito dell'operazione investigativa, diventa cruciale l'acquisizione delle chiavi di cifratura, attività questa la cui realizzazione apre interrogativi di non poco momento, specialmente sotto il profilo della sua compatibilità con il quadro dei diritti fondamentali e delle garanzie processuali riconosciute dal nostro ordinamento.

A complicare ulteriormente le cose concorrono poi due ulteriori fattori che, come ha dimostrato l'ampia casistica giurisprudenziale formatasi sul tema[3], vengono specialmente in rilievo quando la captazione abbia ad oggetto messaggi scambiati via *chat* attraverso l'impiego dei c.d. criptofonini.

Come è noto, con tale espressione si allude a quella particolare tipologia di *smartphone* appositamente modificati per risultare impermeabili ad ogni tentativo di attacco e di intrusione esterna, compresa quella veicolabile attraverso il captatore informatico; si tratta inoltre di dispositivi che, per poter interagire tra loro, sfruttano una piattaforma di comunicazione, che, oltre a fornire un sistema di crittografia particolarmente sofisticato, non sfrutta la rete telematica pubblica ma funziona grazie ad un server gestito da privati, spesso allocato all'estero[4].

---

[3] Cfr., *ex multis*, Cass. pen., Sez. IV, 28 aprile 2023, n. 17647, Gulluni, inedita; Cass. pen., Sez. IV, 18 aprile 2023, Papalia, in C.E.D. Cass., n. 284563-01; Cass. pen, Sez. IV, 5 aprile 2023, n. 16347, in *www.penaledp.it*, Cass. pen., Sez. I, 13 ottobre 2022, Calderon, in C.E.D. Cass., n. 283998 e in *Cass. pen.*, 2023, p. 1432 ss.; Cass. pen., Sez. IV, 18 aprile 2023, n. 16345, Liguori+3, *inedita*; Cass. pen, Sez. I, 15 settembre 2022, n. 34059, Molisso, inedita; Cass. pen., Sez. I, 15 febbraio 2023, n. 6363, Minichino, inedita; Cass. pen., Sez. IV, 7 settembre 2022, n. 32915, in *www.giurisprudenzapenale.it*.

[4] Sin dai primi commenti sul tema, è stata giustamente avvertita come cruciale la definizione delle peculiarità tecniche di questi nuovi dispositivi. Sul punto, si v. W. NOCERINO, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen.*, 2023, p. 1435 ss.; L. FILIPPI, *Criptofonini e diritto di difesa*, in *questa rivista*, 2023, 2, p. 321 ss.; D. CURTOTTI - V. RIZZI - W. NOCERINO - A. RUSSITTO - G. GILIBERTI - G. SCARPA, *Piattaforme criptate e prova penale*, in *Sist. pen.*, 2023, n. 6, p. 173 ss.; M.T. MORCELLA, *La vicenda dei criptofonini in attesa della decisione della Cassazione*, in *Il penalista*, 6 aprile 2023, § 7; A. BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*, in *Giur. Pen. Web*, 2023, n. 2, pp. 1-24; L. LUDOVICI, *I criptofonini: sistemi informatici criptati e server occulti*, in *www.penale.it*, f. 3, 2023, pp. 417-423; G. FIORUCCI, *La vicenda dei criptofonini: le questioni aperte in attesa dell'imminente intervento delle Sezioni Unite*, ivi, 2024, f. 1, pp. 49-60. Sul punto si v. anche G. SPANGHER, *Criptofonini: sono "in gioco" diritti fondamentali*, in *Cass. pen.*, 2024, p. 179, ove l'Autore rileva che, con il passare del tempo, le numerose pronunce intervenute sul tema hanno consentito di portare alla luce aspetti tecnici, inizialmente rimasti ignoti, che si sono ben presto rivelati

Tutto questo insieme di congegni protettivi porta, come detto, a due ulteriori profili di criticità che gravano sull'attività di ricerca della prova: l'uno legato alla necessità, per gli investigatori, di direzionare l'azione intrusiva del captatore informatico non verso il singolo dispositivo ma verso il server centrale, indiscusso "tallone d'Achille" di un circuito comunicativo altrimenti insondabile; l'altro, che, invece, deve essere riferito alla difficoltà fino ad oggi riscontrata in giurisprudenza di mettere opportunamente a fuoco l'esatta natura giuridica dell'attività di decodificazione dei messaggi e dei flussi comunicativi criptati.

Ma se il quadro finora tratteggiato rende non certo facile la vita all'interprete che tenti di ricostruire lo statuto giuridico di queste attività tecnico-investigative evidentemente prive di una chiara e specifica regolamentazione nel contesto normativo attualmente vigente, non vi è dubbio che l'impresa si faccia ancora più ardua laddove il materiale probatorio in questione, dapprima acquisito all'estero, faccia poi il suo ingresso nei procedimenti italiani per il tramite di un ordine europeo di indagine.

Ebbene, come è noto, proprio questo è il sostrato fattuale di un importantissimo dittico di sentenze recentemente depositate dalle Sezioni Unite della Corte di cassazione[5] con le quali è stato affermata la piena utilizzabilità della messaggistica acquisita autonomamente all'estero nell'ambito di distinti procedimenti domestici e poi riversata, sotto forma di materiale probatorio già perfettamente selezionato e decriptato, nei procedimenti italiani, in esecuzione di ordini europei di indagine emessi dai pubblici ministeri procedenti

Naturalmente, tra le varie questioni affrontate e risolte dalla Suprema Corte figurano anche quelle cui si è fatto più sopra riferimento ed è al loro approfondimento che è dedicato il presente contributo.

## 2. I *criptofonini*: il problema delle intercettazioni *omnibus*

Procedendo con ordine, la prima questione riguarda le modalità attraverso le quali la messaggistica sarebbe stata intercettata; ed il condizionale è d'obbligo perché nemmeno le Sezioni Unite sono state in grado di dire se la captazione occulta sia avvenuta contestualmente alla comunicazione ovvero in un momento ad essa successivo, e quindi attingendo dati telematici *freddi*[6]. Sta di fatto che, per

"molto significativi e illuminanti" per comprendere la natura e i contenuti delle procedure poste in essere.

[5] Cass. pen., Sez. Un. 29 febbraio 2024, (dep. 14 giugno 2024), n. 23756 – Pres. Cassano – Rel. Corbo – P.M. Gaeta (conf.) - Sez. Un. 29 febbraio 2024 (dep. 14 giugno 2024), n. 23755 – Pres. Cassano – Rel. Corbo – P.M. Giordano, in *www.penaledp.it*, 21 ottobre 2024, con nota di O. MURRO - W. NOCERINO, *Più ombre che luci nelle sentenze delle Sezioni Unite sui criptofonini*, e in *Cass. pen.*, 2024, p. 2575 ss. con nota di A. NAPPI, *Le Sezioni Unite sui criptofonini: plus dixerunt quam voluerunt?*

[6] Rilevano condivisibilmente O. MURRO - W. NOCERINO, *Più ombre che luci, cit.*, p. 9, «la Corte sembra disinteressarsi della natura delle attività di indagine che, a monte, avevano consentito di penetrare all'interno delle piattaforme di comunicazione criptate: non è dato sapere in che modo

i connotati tecnici dei criptofonini, se intercettazione vi è stata, questa è senz'altro avvenuta attraverso l'inoculazione di un captatore informatico nel *server* di supporto della piattaforma Sky-ECC.

Ebbene, qual è il problema di questa modalità attuativa? Che ha pacificamente comportato una intercettazione "di massa" a danno di tutti gli utenti del servizio; il punto è, quindi, capire se all'interno del nostro ordinamento possa essere considerata utilizzabile una prova così formata.

La risposta affermativa viene dalle Sezioni Unite seconde le quali si tratterebbe di materiale acquisito nel rispetto dei diritti fondamentali riconosciuti dal nostro ordinamento giuridico perché tutti i soggetti intercettati, servendosi di un servizio di comunicazione ripetutamente utilizzato da organizzazioni criminali insediate in vari Stati e dedite al traffico anche internazionale di sostanze stupefacenti, risultavano attinti da elementi indizianti circa il loro coinvolgimento nella commissione di gravi reati, in particolare in materia di traffico di sostanze stupefacenti. Da questa premessa, il *plenum* fa discendere la conclusione che non ci troveremmo in presenza di una intercettazione generalizzata e indiscriminata.

Ebbene, la conclusione lascia alquanto perplessi perché il rispetto dell'art. 15 Cost. presuppone pacificamente che vi sia un collegamento - di cui la motivazione del decreto autorizzativo deve dare conto – tra il soggetto cui fa capo l'utenza intercettata e gli specifici reati oggetto del procedimento nel quale l'intercettazione è disposta. Evidente, dunque, che tale collegamento non ricorre quando l'autorizzazione venga giustificata, come nella ricostruzione delle Sezioni Unite, sulla base di generiche congetture circa il possibile coinvolgimento degli intercettati nella commissione di fatti di reato che, oltre ad essere diversi da quelli in relazione ai quali si sta indagando, non è dato sapere neppure se siano stati o meno realmente individuati, anche solo a livello di mera *notitia criminis*.

Ma se quindi tali intercettazioni sono state realizzate nel procedimento *a quo* con modalità tali da confliggere con il parametro costituzionale di riferimento, la loro utilizzabilità deve essere esclusa anche nel procedimento *ad quem* essendo, peraltro, indubbio – come chiarito fin dal 2004 con la sentenza Esposito - che la circolazione tra procedimenti dei risultati delle intercettazioni ex art. 270 c.p.p. presuppone la legittimità dell'attività intercettiva svolta *ab origine*[7].

---

si sia giunti all'acquisizione dei messaggi criptati, se attraverso la captazione di flussi in fase dinamica ovvero mediante l'acquisizione di dati telematici freddi, cioè già archiviati nella memoria del server, oppure procedendo ad un'apprensione *omnibus*».

[7] Come hanno da tempo le Sezioni Unite della Corte di cassazione (Cass. pen., Sez. Un., 17 novembre 2004, p.m. in proc. Esposito, in *C.E.D Cass.*, n. 229244-01) «Il procedimento di ammissione dell'intercettazione rimane del tutto estraneo alla disciplina dell'utilizzazione dei suoi risultati in un diverso giudizio. Ma questo non può significare affatto che nel giudizio *ad quem* sia indifferente la legalità del procedimento di autorizzazione ed esecuzione delle intercettazioni. Se la violazione della garanzia di libertà e segretezza delle comunicazioni può

Conclusione questa che vale anche nel caso specifico preso in esame dalle Sezioni Unite atteso che la presunzione *relativa* di conformità (richiesta dall'art. 1 par. 4 della Direttiva 2014/41/UE) ai diritti fondamentali riconosciuti nello Stato di emissione che si ritiene assista le prove allogene[8] è destinata però a sgretolarsi nel momento in cui emerga *ex actis* che tale conformità in realtà sia insussistente. Senza contare che, in base al già richiamato principio affermato dalle Sezioni Unite Esposito, l'utilizzabilità delle *chat* deve essere esclusa anche perché l'atto di indagine richiesto con l'O.E.I. non sarebbe consentito in un caso interno analogo.

### 3. *Segue*: acquisizione dell'algoritmo e violazione del domicilio digitale

Possiamo a questo punto passare ad affrontare il secondo aspetto problematico, quello concernente l'acquisizione dell'algoritmo necessario per decriptare le *chat* sulla piattaforma Sky-ECC. Come per molti aspetti di questa vicenda, anche in proposito c'è tutt'ora molto poca chiarezza. Quello che è certo è però che, anche in questo caso, un ruolo decisivo è stato svolto dal captatore informatico che – secondo l'opinione maggiormente accreditata – avrebbe fatto partire dal *server* una notifica autoinstallante verso ciascun dispositivo, consentendo così agli investigatori di entrare, tra l'altro, in possesso di tutti gli algoritmi necessari per decriptare le *chat*.

Ora, se è indubbio che attraverso questa modalità si sia operata una intrusione nel domicilio informatico degli utenti, le Sezioni Unite affermano comunque la piena compatibilità dell'operazione con il nostro ordinamento. Questo perché il captatore informatico, pur avendo operato al di fuori di quanto previsto dalla legge – l'art. 266 c. 2 e c. 2 bis c.p.p., che ne disciplinano l'inserimento nel dispositivo portatile e non nel *server* – non costituirebbe un mezzo atipico di indagine o di prova, bensì uno strumento tecnico necessario per il compimento dell'intercettazione, mezzo di ricerca della prova tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost. con il quale il principio di inviolabilità del domicilio deve necessariamente coordinarsi, subendo la necessaria compressione (al pari dell'art. 15 Cost.).

---

rendere inutilizzabile la prova nel giudizio a quo, a maggior ragione deve poter rendere inutilizzabile la prova nel giudizio *ad quem*, nel quale ha più ristretti limiti di ammissibilità».

[8] Come ricordato dalle stesse Sezioni Unite, il principio della presunzione di legittimità dell'attività compiuta all'estero ai fini dell'acquisizione di elementi istruttori è oggetto di costante e generale enunciazione da parte della giurisprudenza della Corte di cassazione: cfr., *ex plurimis*, Cass. pen., Sez. VI, n. 44882, 4 ottobre 2023, Barbaro, in C.E.D. Cass., n. 285386; Cass. pen, Sez. III, n. 1396, 12 ottobre 2021, Torzi, ivi, n. 282886; Cass. pen., Sez. IV, n. 19216, 6 novembre 2019, Ascone, ivi, n. 279246.

A conferma della ricostruzione offerta, la Suprema Corte richiama l'analogo principio affermato dalla giurisprudenza di legittimità[9] in tema di posizionamento occulto di microspie all'interno di ambienti di privata dimora.

Ebbene, a parte il fatto che le intercettazioni che implicano anche l'intrusione nel domicilio sono soggette, per legge, ad una disciplina rafforzata proprio per il loro carattere multi-lesivo, a riprova del fatto che l'intervento del legislatore per disciplinare la peculiare fattispecie qui considerata appare ancora più doveroso. Il punto però che è che servirsi del captatore informatico per carpire le chiavi di cifratura è un tipo di attività affatto diversa dall'intercettazione: qui, infatti, non si tratta di captare clandestinamente i contenuti delle comunicazioni; qui si tratta di acquisire un dato informatico contenuto nella memoria del dispositivo, penetrando clandestinamente all'interno di esso, cioè nel domicilio informatico dell'utente.

E non si può nemmeno dire che si tratta di una attività prodromica all'intercettazione, come correttamente sostenuto in materia di posizionamento delle microspie, perché l'attività captativa consiste e si esaurisce nella registrazione dei flussi comunicativi; le chiavi di cifratura non servono per registrare le comunicazioni, servono per renderle intellegibili che è però attività successiva e quindi estranea all'intercettazione.

Una volta chiarito questo, non credo che si possa più dubitare che ci troviamo al cospetto di un mezzo di ricerca della prova atipico. Allo stesso tempo, è un mezzo di indagine senz'altro incidente su diritti fondamentali della persona perché, suo tramite, si determina il sacrificio dell'inviolabilità del domicilio, oltre ad essere strumentale alla violazione della segretezza delle comunicazioni.

Ma se così è allora non pare peregrino concludere che il suo utilizzo non possa trovare cittadinanza nel nostro ordinamento senza un apposito intervento normativo che contempli e disciplini tale tipo di attività *extra ordinem*.

## 4. *Segue*: stringhe informatiche, chiavi di cifratura e diritto al contraddittorio "per la prova"

L'ultimo punto che qui si intende affrontare è se sia o meno indispensabile che le difese dispongano delle stringhe informatiche registrate e degli algoritmi utilizzati per decriptarle.

Sappiamo che, nella vicenda all'esame delle Sezioni Unite, le autorità francesi avevano trasmesso le *chat* già decriptate e nulla di più. Sappiamo inoltre che la Suprema Corte esclude che l'indisponibilità dell'algoritmo di decriptazione costituisca di per sé una violazione dei diritti fondamentali considerato che, per l'attuale scienza informatica, il pericolo di alterazione dei

[9] Cfr., *ex plurimis*, Cass. pen., Sez. II, 13 febbraio 2013, in C.E.D Cass., n. 255541; Cass. pen., Sez. I, 2 ottobre 2007, ivi, n. 238108.

dati, fatto salvo il diritto alla prova contraria, non sussisterebbe. Abbiamo cioè due sole alternative possibili: la chiave o è quella giusta e allora il messaggio viene messo "in chiaro", o è quella sbagliata e allora il tentativo di decriptazione fallisce del tutto; *tertium non datur.*

Quanto poi all'indisponibilità delle registrazioni contenenti la messaggistica "allo stato grezzo", le Sezioni Unite escludono la violazione dell'art. 6 par. 1 lett. b), della Direttiva 2014/41/UE - secondo cui l'O.E.I. può essere emesso soltanto se l'atto di indagine richiesto avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo - atteso che il deposito dei verbali e delle registrazioni, pur previsto dall'art. 270 c.p.p. – che rappresenta l'atto di indagine omologo cui occorre fare riferimento a livello interno -, non figura tra le condizioni per l'acquisizione dei risultati di intercettazioni disposte in altro procedimento ma rileva in una fase successiva e di controllo, e la sua attuazione può essere anche differita a dopo la conclusione delle indagini senza precludere l'utilizzazione degli esiti delle captazioni ai fini cautelari.

Il ragionamento della Corte sembra esporsi ad almeno due rilievi critici.

Il primo riguarda la riferita irrilevanza, ai sensi dell'art. 6, delle garanzie procedimenti di cui all'art. 270. Infatti, nel contesto della disposizione nazionale esaminata, tanto il presupposto oggettivo, concernente il reato per il quale si procede nel procedimento *ad quem*, tanto il deposito dei verbali e delle registrazioni, hanno il medesimo peso ed assumono rilevanza in un'unica ed identica prospettiva: ai fini dell'utilizzabilità dei risultati delle intercettazioni allogene. Ne discende dunque che risulta alquanto arbitrario e disallineato rispetto al dettato normativo ritenere che soltanto l'attinenza del procedimento *ad quem* ad un reato procedibile d'ufficio rientri tra le condizioni richieste per il compimento dell'atto di indagine in un caso interno analogo e non anche il concorrente requisito ancorato alla disponibilità per le parti dei verbali e delle registrazioni.

Né a favore della diversa conclusione milita il fatto che il deposito possa essere differito, visto che si tratta di una eventualità eccezionale che presuppone la sussistenza di un presupposto specifico – rischio di un grave pregiudizio per le indagini a seguito dell'avvenuto deposito – senza il quale non è possibile derogare alla regola generale cui l'atto di indagine richiesto deve quindi conformarsi[10].

[10] Di questo avviso sembra essere anche G. SPANGHER, *Criptofonini: sono in gioco,* cit., p. 179, che, infatti, all'indomani della rimessione al *plenum* dei ricorsi in materia di utilizzabilità dei criptofonini, denunciava che «il quesito davanti alla Corte di cassazione a Sezioni Unite va integrato con questi aspetti, essendo necessario consentire nel contraddittorio anche attraverso l'analisi dei provvedimenti delle autorità francesi (ormai a disposizione della magistratura italiana) una verifica di questi profili (la chiave di decrittazione in primis che nel caso Sky ECC non è coperta dal segreto) che sono alla base dei provvedimenti impugnati dagli imputati al fine di verificarne l'utilizzabilità»

Ma anche volendo per assurdo ammettere che, a fini cautelari, il deposito delle registrazioni, e quindi delle chiavi di cifratura, possa essere bypassato, questo non fa che rinviare il problema, posticipandolo ad una fase successiva, quella del giudizio, e con effetti ancora più dirompenti.

L'art. 431 c. 1 lett. b e d) c.p.p. dispone che entrano nel fascicolo dibattimentale gli atti di indagine, anche acquisiti mediante rogatoria internazionale o ordine europeo di indagine, che presentano natura irripetibile.

Proiettata sulla materia delle intercettazioni, la regola implica che, oltre alle chiavi di cifratura, in quanto documenti informatici, entrano nel fascicolo per il dibattimento le registrazioni, le c.d. bobine o comunque i supporti digitali dove i flussi comunicativi sono memorizzati in quanto atti irripetibili. Quanto invece alla decriptazione, questa – ecco il punto cruciale - non è atto irripetibile: è come la traduzione in lingua italiana di conversazioni svolte utilizzando un idioma diverso dal nostro, è, cioè, atto ripetibile, che come tale dovrà essere assunto in dibattimento, nel contraddittorio delle parti, con le forme della perizia.

Immaginiamo però che, una volta giunti ad un ipotetico dibattimento, venga omesso il deposito e l'acquisizione delle registrazioni al fascicolo del dibattimento. Immaginiamo ancora che queste chiavi di cifratura non vengano mai consegnate e, ciononostante, accada che le *chat* decriptate all'estero finiscano ciononostante per entrare a far parte del patrimonio gnoseologico materialmente conoscibile dall'organo giudicante.

La domanda che, in un simile scenario, si pone è: il giudice potrà spingersi anche ad utilizzare questo materiale probatorio per decidere sulla responsabilità dell'imputato e, se del caso, a condannarlo? Ebbene, in un sistema dove la prova si forma in dibattimento e dove le eccezioni a questa regola aurea sono tassative e costituzionalmente presidiate, la risposta negativa sembrerebbe scontata, considerando che le registrazioni e gli algoritmi di decriptazione, sebbene in possesso delle autorità straniere, non sono stati fatti oggetto di trasmissione. Ciononostante, le Sezioni Unite non sembrano ravvisare in ciò un problema e allora è lecito pensare che quello verso cui stiamo andando è probabilmente un processo penale più efficiente ma, allo stesso, è anche un processo penale che rischia di essere sempre meno giusto.