I CRIPTOFONINI: SISTEMI INFORMATICI CRIPTATI E SERVER OCCULTI*

Luigi Ludovici

1. I criptofonini: due (doverose) premesse tecniche

La comparsa dei "criptofonini" tra i mezzi in dotazione della criminalità, specialmente di quella organizzata, ha portato alla messa in campo di metodi investigativi dotati di capacità pervasive così intense da aprire un nuovo e delicatissimo fronte all'interno del già incandescente dibattito sui rapporti tra i tradizionali mezzi di ricerca della prova e le nuove tecnologie.

I "criptofonini", infatti, rappresentano il *non plus ultra* offerto oggi dalla scienza e dalla tecnica in fatto di

segretezza e di sicurezza delle comunicazioni. In particolare, si tratta di comuni *smartphone* sui quali però sono state apportate numerose modifiche, soprattutto a livello di software, tali da renderli impermeabili ad ogni forma di intrusione esterna da parte di terzi. Non fa eccezione neppure il captatore informatico che qui trova sbarrate tutte le sue consuete via d'accesso: nei criptofonini risultano, infatti, disattivati i servizi Google, la videocamera, il microfono, il sistema Bluetooth, la porta USB, il sistema di geolocalizzazione.

Come se non bastasse, questi dispositivi non sono agganciati alla tradizionale rete telefonica o telematica in quanto, per comunicare, si servono di piattaforme informatiche crittografate il cui funzionamento dipende dall'impiego di server gestiti da privati, spesso allocati all'estero. Da qui, la necessità di disporre delle chiavi di cifrature in assenza delle quali, i flussi comunicativi scambiati tramite i criptofonini si presentano come mere stringhe informatiche redatte secondo il sistema binario: cioè a dire, sequenze di numeri prive di qualsiasi significato intellegibile ai più.

Un così composito e sofisticato sistema di protezione delle comunicazioni[1] non è però riuscito ad evitare che, tra il 2020 e il 2021, si arrivasse alla decrittazione e al conseguente smantellamento di due delle principali piattaforme criptate fino a quel momento conosciute, la Encrochat e la Sky ECC. Questo formidabile successo investigativo, raggiunto grazie all'impiego di squadre investigative di indagine costituite dalle autorità francese, olandese e belga, ha avuto un impatto enorme anche nell'ambito dei procedimenti di criminalità organizzata pendenti in Italia. Infatti, le Procure italiane hanno, di riflesso, emesso una "pioggia" di ordini europei di indagine volti all'acquisizione, per il tramite dell'autorità giudiziaria francese, dei dati comunicativi ritenuti di interesse per l'accertamento dei reati perseguiti nei singoli procedimenti. Ne è, quindi, scaturita una sequela di provvedimenti cautelari che nel corso degli ultimi mesi hanno generato, a cascata, altrettante pronunce della Corte di Cassazione[2].

Ebbene, in linea di prima approssimazione, sembra che si possa convenire sul fatto che la provenienza di questa enorme quantità di materiale probatorio da uno strumento di cooperazione giudiziaria qual è l'O.E.I. abbia in parte fatto come da cortina di fumo, dando cioè modo alla giurisprudenza di legittimità di disinteressarsi – più a torto che a ragione - della natura e della legittimità delle attività di indagine che, a monte, avevano consentito di penetrare all'interno delle piattaforme di comunicazione criptate. In particolare, non è dato sapere in che modo 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. A questo proposito, l'unico dato fornito dalla giurisprudenza è che i messaggi sarebbero stati decrittati perché la società che ne era proprietaria avrebbe messo a disposizione degli investigatori gli algoritmi e le chiavi di cifratura.

Tale spiegazione, però, oltre a non giustificare il disinteresse per il tipo di attività investigativa che a monte aveva consentito l'acquisizione dei dati, appare comunque del tutto implausibile in punto di fatto. Non si deve, infatti, dimenticare che i criptofonini attenzionati usavano il sistema di crittografia *end to end* che, a differenza di quello denominato *pin to pin*, si serve di chiavi di cifratura depositate non all'interno del server ma direttamente nei dispositivi[3]: ciò significa che non è tecnicamente possibile che la società proprietaria del server abbia potuto fornito agli investigatori l'algoritmo per decriptare le stringhe informatiche, trattandosi di un dato ad appannaggio esclusivo degli utenti del servizio cioè i proprietari dei *devices*.

Per questo motivo sembra da condividere la tesi – avanzata in dottrina[4] – secondo la quale la captazione dei flussi comunicativi in questione sarebbe avvenuta in questo modo: attraverso l'inoculazione di un *malware* all'interno del server per il successivo invio di una notifica *push* – che cioè perviene al destinatario senza bisogno di *download* – verso i criptofonini che, quindi, dialogando con il server di gestione, avrebbero automaticamente trasmesso le chiavi di cifratura agli investigatori.

Partendo da queste premesse di ordine tecnico, scopo del presente contributo è quello di analizzare i problemi giuridici che circondano i diversi possibili scenari investigativi connessi all'impiego dei criptofonini; con l'avvertimento però, che il sistema di comunicazione criptata posto alla base delle attività di indagine che qui si intende prendere in esame è da intendersi come facente capo ad un server fisicamente allocato su territorio italiano, come tale non interessato dalle questioni connesse all'impiego dell'O.I.E. delle quali pertanto in questa sede non verrà dato conto.

2. Le attività di apprensione dei dati digitali: le intercettazioni telematiche

La prima possibilità è che il captatore informatico installato nel *server* abbia captato in tempo reale le *chat* e i flussi comunicativi gestiti dalle piattaforme criptate. La contemporaneità tra la captazione e la comunicazione induce a ricondurre la prima nel concetto di intercettazione e, in particolare, di intercettazione telematica di cui all'art. 266-bis c.p.p.

Ora, rispetto a questa eventualità, non sembra che il problema sia tanto il fatto che la legge disciplina l'utilizzo del captatore solo come strumento di intercettazione ambientale da installarsi su dispositivi portatili e non anche su dispositivi fissi, come appunto il server. Infatti, nella fattispecie esaminata, l'utilizzo del captatore informatico non presenta comunque alcun rischio di violare indiscriminatamente la riservatezza del domicilio: ad essere captati infatti sono necessariamente i flussi comunicativi scambiati tra due dispositivi

portatili e non le conversazioni tra presenti; ragion per cui, da questo punto di vista, il captatore informatico si sottrae alla speciale disciplina di cui all'art. 266 c. 2-bis – non generando quei rischi che la stessa è preordinata a scongiurare[5] – per ricadere pertanto nella sfera applicativa della normativa di carattere generale.

Con questo non si vuole naturalmente dire che il particolare tipo di attività di ricerca della prova qui esaminato non presenti criticità. Anzi.

Non dobbiamo infatti dimenticare che, una volta che il *server* sia stato "bucato", la captazione riguarderà non solo le comunicazioni e le conversazioni ritenute potenzialmente rilevanti nel procedimento ove l'intercettazione sia stata disposta, ma anche tutti i flussi comunicativi intercorsi tra gli abbonati al servizio: cadute le barriere protettive, davanti agli investigatori si apre quindi una distesa sterminata di materiale probatorio acquisito attraverso il monitoraggio di una moltitudine di utenze di cui, nel provvedimento autorizzativo, non era però stata fatta alcuna menzione e rispetto alle quali, dunque, non era stato compiuto il doveroso vaglio circa la necessità di sacrificarne la riservatezza.

Ebbene, almeno fino a quando, sul piano strettamente tecnico, non risulti possibile limitare il controllo occulto ai soli flussi comunicativi di interesse per il procedimento in corso, non sembra che un simile *modus procedendi* possa trovare cittadinanza nel nostro ordinamento. Se, infatti, la legge consente di violare la riservatezza di quelle comunicazioni rispetto alle quali sussistono determinati presupposti giustificativi, non si vede come un giudice possa autorizzare un'attività di intercettazione (telematica) nella consapevolezza che, così facendo, sta automaticamente consentendo la captazione a tappeto di tutti i flussi comunicativi veicolati dal *server* infettato e tutto questo in assenza dei necessari requisiti stabiliti dalla legge[6].

Laddove poi questa soluzione dovesse apparire troppo radicale, l'unica alternativa possibile – a dati normativi immutati – sembra quella di accontentarsi di una tutela postuma, imperniata sull'inutilizzabilità ex art. 271 c.p.p. dei flussi comunicativi diversi da quelli rispetto ai quali l'intercettazione era stata richiesta e autorizzata.

Conclusione questa che, *a fortiori*, deve valere anche nel caso in cui i medesimi risultati captativi vengano fatti addirittura rifluire, ex art. 270 c.p.p., in un procedimento diverso da quello nel quale l'intercettazione – mediante inoculazione del captatore all'interno del server - era stata originariamente disposta, per fatti ivi non perseguiti e che magari, al momento della captazione, non erano ancora conosciuti neppure a livello di

notitia criminis: Infatti, a prescindere da se il reato oggetto del procedimento *ad quem* preveda o meno l'arresto obbligatorio in flagranza, il punto è che la circolazione tra procedimenti dei risultati delle intercettazioni presuppone, quale suo requisito base - che, per le ragioni illustrate, difetta rispetto ai flussi comunicativi diversi da quelli riferibili all'utenza-bersaglio indicata nel decreto autorizzativo – quello della legittimità dell'attività intercettiva svolta a monte, nel procedimento *a quo*[7].

3. *Segue*: il sequestro di documenti informatici

Come già ricordato, è anche possibile che gli investigatori acquisiscano le chat e i flussi comunicativi recuperandoli dalla memoria del server. In questo caso, non avendo a che fare con comunicazioni in corso di svolgimento, e quindi con captazioni *live*, certamente ci troviamo al di fuori del concetto di intercettazione.

Se su questo non ci sono dubbi, è altrettanto vero che, per poter correttamente classificare, da un punto di vista giuridico, questa attività dobbiamo prima interrogarci sulla natura del materiale probatorio raccolto.

A questo proposito, si deve notare che, nel momento in cui i dati acquisiti non sono il risultato di una captazione occulta fatta dagli investigatori ma rappresentano l'oggetto di una attività di archiviazione operata dal server per ragioni di funzionamento e di gestione del servizio, i supporti digitali che incorporano le chat, i file audio o video, non ineriscono all'attività di indagine, e quindi non sono atti del procedimento; al contrario, essi si qualificano come documenti informatici, come tali suscettibili di sequestro probatorio laddove costituenti corpo del reato o cose ad esso pertinenti.

Chiarito ciò, conviene però fare un piccolo passo indietro perché, specialmente nel caso in cui l'ingresso nel *server* sia stato effettuato non con l'assenso della società che lo gestisce ma attraverso l'impiego di un malware, si pone il problema di verificare la legittimità di un simile operato

Infatti, se non altro quando il *server* venga occultamente penetrato, questa intrusione integra un atto di perquisizione informatica che però, essendo stata condotta clandestinamente, deve considerarsi illegittima perché svolta senza le garanzie previste dalla legge. Se a questo poi aggiungiamo che la memoria del server rappresenta a tutti gli effetti il domicilio informatico di ciascun utente relativamente ai dati digitali che lo riguardano, anche il rischio che il problema venga aggirato facendo leva sulla sfuggente categoria della prova atipica sembra in realtà scongiurato; infatti, la prova atipica, proprio in quanto tale, risulterebbe inidonea a comprimere valori che, al contrario, sono presidiati dalla riserva di legge, come appunto il domicilio,

compreso quello informatico[8].

Detto questo, è però anche vero che, laddove l'attività in questione venisse comunque espletata, sarà difficile riuscire ad escludere l'utilizzabilità dei dati acquisiti in forza del successivo sequestro; e ciò per il noto principio – che a tutt'oggi, se non altro a livello giurisprudenziale, gode di ottima salute - del *male captum bene retentum**[9]***.

4. L'attività di decriptazione

Quanto all'attività di decriptazione, è emerso come, per l'acquisizione delle chiavi di cifratura depositate presso i criptofonini, l'unica strada ipotizzabile sia quella di far partire dal server infettato una notifica push, attività questa che, ad avviso della dottrina, darebbe luogo ad una forma di acquisizione probatoria illegittima perché lesiva della libertà morale dei soggetti coinvolti[10]. A ben guardare però, la denunciata violazione dell'art 188 c.p.p. appare in questo caso più apparente che reale: infatti, qui a collaborare involontariamente con gli investigatori non è tanto l'utente del servizio, che infatti non è neppure chiamato a scaricare il messaggio di notifica, ma piuttosto è il criptofonino stesso che, interfacciandosi con il server, disvela automaticamente le proprie chiavi di cifratura.

Detto questo, non sembra revocabile in dubbio che l'algoritmo impiegato per decrittare i flussi comunicativi captati o comunque sequestrati all'interno del server debba essere messo senz'altro a disposizione delle parti unitamente alle stringhe informatiche non ancora decriptate. In assenza di questi dati, infatti, non si vede come sia possibile esercitare a pieno il diritto di difesa su un tema di fondamentale importanza qual è quello della piena corrispondenza tra il testo originario (i.e., la stringa informatica) e il testo intelleggibile introdotto come prova nel giudizio[11]. Senza contare che, quando i flussi comunicativi siano stati acquisiti tramite captazioni *live*, la transizione dei dati telematici dal linguaggio binario delle stringhe ad un linguaggio intellegibile, non integrando certo una operazione irripetibile, sembra destinata a trovare ingresso nel fascicolo dibattimentale non certo sotto forma di brogliaccio di p.g. ma necessariamente con le forme garantite e, di regola, ineludibili della perizia.

** Contributo tratto dalla relazione svolta nell'ambito del convegno "Per uno statuto dei nuovi mezzi di ricerca della*

prova di fronte alla società digitale", tenutosi in Roma in data 22.9.2023.

---

[1] Per una più ampia ed approfondita disamina delle specifiche tecniche che caratterizzano questi dispositivi, si v. Nocerino, L'acquisizione della messaggistica, cit., p. 1433 ss.

[2] Cfr., Cass., Sez. IV, 28 aprile 2023, n. 17647, Gulluni, inedita; Cass., Sez. IV, 18 aprile 2023, Papalia, in C.E.D. Cass., n. 284563-01; Cass., Sez. IV, 5 aprile 2023, n. 16347, in www.penaledp.it; Cass., Sez. I, 13 ottobre 2022, Calderon, in C.E.D. Cass., n. 283998 e in *Cass. pen.*, 2023, p. 1432 ss.; Cass., Sez. IV, 18 aprile 2023, n. 16345, Liguori+3, *inedita*; Cass., Sez. I, 15 settembre 2022, n. 34059, Molisso, inedita; Cass., Sez. I, 15 febbraio 2023, n. 6363, Minichino, inedita; Cass., Sez. IV, 7 settembre 2022, n. 32915, in *www.giurisprudenzapenale.it*. Quanto alla dottrina finora intervenuta sul tema, si v. Nocerino, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen*., 2023, p. 1435 ss.; Filippi, *Criptofonini e diritto di difesa*, in *questa rivista*, 2023, 2, p. 321 ss.; Curtotti-Rizzi-Nocerino-Russitto-Giliberti-Scarpa, *Piattaforme criptate e prova penale*, in *Sist. pen*., 2023, n. 6, p. 173 ss.; Morcella, *La vicenda dei criptofonini in attesa della decisione della Cassazione*, in *Il penalista*, 6 aprile 2023, § 7; 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.

[3] Per un chiarimento in proposito, si v., *ex multis*, Cass., Sez. I, 13 ottobre 2022, in *C.E.D Cass*., n. 283998-01, ove, appunto, la Suprema Corte precisa che "Tali sistemi di comunicazione di Sky Ecc non sono però basati sulla tecnologia *pin to pin* (tipo Blackberry, cioè su un sistema crittografico dove le chiavi di cifratura sono collocate in un server), bensì sul sistema *end to end*, colloquiano, sicché, in questa modalità, neanche il gestore del servizio è in grado di conoscere le chiavi utilizzate e, di conseguenza, il contenuto delle comunicazioni".

[4] Cfr. Filippi, *Criptofonini e diritto di difesa*, in *questa rivista*, 2023, n. 2, p. 324 ss.

[5] In proposito, cfr. Cass., Sez. Un., 28 aprile 2016, Scurato, in *C.E.D. Cass*., n. 266905-01.

[6] In senso sostanzialmente conforme, Siracusa, Il Giano bifronte: autorità e libertà nella data retention. A proposito di una recente pronuncia della Corte di cassazione, in Arch. Pen., 2023, 2, p. 9; Curtotti-Rizzi-

Nocerino-Russitto-Giliberti-Scarpa, *Piattaforme criptate e prova penale*, in *Sist. pen*., 2023, n. 6, 185; Filippi, *sub art. 266 bis*, in Giarda-Spangher (a cura di), *Codice di procedura penale commentato*, Milano-Padova, 2023; Mancuso, *L'acquisizione di contenuti e-mail*, in Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, p. 5156 ss.

[7] Come hanno da tempo le Sezioni Unite della Corte di Cassazione (Cass., 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 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] Sul punto, si v. Bronzo, *L'impiego del* trojan horse *informatico nelle indagini penali*, in *Rivista italiana per le scienze giuridiche*, 8/2017, p. 348.

[9] Per l'affermazione del principio, si v. Cass., Sez. Un., 16 maggio 1996, Sala, in *Cass. pen*., 1996, p. 3268 ss.

[10] E' di questo avviso Filippi, *Criptofonini e diritto di difesa, cit*., p. 326.

[11] Nella sentenza Cass., Sez. I, 6 aprile 2023, n. 16347, in www.penaledp.it, la Suprema Corte, nelll'escludere che ricorre la dedotta violazione del diritto di difesa per per l'impossibilità di verificare la corrispondenza del dato oridnale con quello trasmesso, rileva che, anche nel caso dei criptofonini, vale il principio giurisprudenziale affermato in materia di decriptazione della messaggistica con sistema Blackberry (quindi, "pin to pin" e non "end to end, come nella specie) secondo il quale "l'uso dell'algoritmo esclude la possibilità di alterazioni o manipolazioni dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici e concreti elementi di segno contrario (sez. 4, n. 30395 del 21/4/2022, Chianchiano, Rv. 283454; sez. 6, n. 14395 del 27/1172019, dep. 2020, Testa, Rv. 275534)". A questo proposito, non ci si può però esimere dal rilevare che, su un piano squisitamente logico, non ha alcun senso gravare la difesa dell'onere di allegare l'inesattezza di un giudizio di identità tra due dati (*i.e.*, quel giudizio che dovrebbe descrivere il rapporto che intercorre tra il testo introdotto in giudizio, da un lato, e il risultato effettivamente ricavabile dalla stringa informatica una volta decriptata, dall'altro) se, al contempo, gli si nega la possibilità di conoscere sia il dato *grezzo* da comparare (*i.e*., la stringa informatica) sia lo strumento necessario per rendere quel dato idoneo alla comparazione (*i.e*., l'algoritmo).