di Lorenzo Savastano*

UTILIZZO INVESTIGATIVO DI DATI SCAMBIATI CON CRIPTOFONINI ENCROCHAT E SKY ECC: LA CASSAZIONE FORNISCE LA "CHIAVE" DI ACCESSO

È una delle tendenze più interessanti osservate negli ultimi anni nel comportamento delle più perverse e ramificate organizzazioni criminali del mondo (Italia compresa): l'impiego di *criptofonini*, soprattutto di fabbricazione *Encrochat* e *SKY ECC*, ovvero device in grado di criptare le comunicazioni tra affiliati, rendendole di fatto "*invisibili*" ai tradizionali strumenti investigativi in uso alle forze di polizia. Quando sono state "*bucate*", le piattaforme di criptazione si sono rivelate una miniera di informazioni incredibile non solo per le indagini, ma anche per una comprensione più lucida e profonda del mondo della criminalità. Ed è proprio sul tema strategico della corretta interpretazione processuale e piena valorizzazione operativa delle informazioni decriptate che si è incentrata la recente Sentenza n. 6364/2023, dello scorso 15 febbraio, della Corte di Cassazione: una vera e propria "chiave" di accesso all'oscuro mondo dei sistemi di criptazione delle comunicazioni.

1. Criptofonini: un nuovo trend criminale

Lo scorso 8 giugno 2021 è stata, a suo modo, una data epocale nella storia delle moderne investigazioni di polizia giudiziaria. Quel giorno, il *Federal Bureau of Investigation* (FBI), la *Politie* olandese, la *Polizei* svedese, in cooperazione la US *Drug Enforcement Administration* (DEA), la *Federal Police* australiana e con il supporto di Europol, hanno infatti concluso l'operazione TROJAN SHIELD/GREENLIGHT, con l'arresto di 800 criminali ed il sequestro, tra l'latro, di oltre 8 tonnellate di cocaina, 22 tonnellate di *cannabis*, 250 armi da fuoco ed oltre 48 milioni di dollari in varie valute mondiali e criptovalute[1]. L'equivalente di anni di indagine.

Nello specifico, l'operazione nasce nel 2019, quando il FBI segretamente sviluppa un potente ed avanguardistico servizio di criptazione delle telecomunicazioni, denominato ANOM, che rapidamente viene acquistato ed utilizzato dalle principali organizzazioni criminali operative su scala mondiale[2]. L'intera operazione si è quindi basata su un espediente semplice, benché ardito ed innovativo, che ha fatto leva su una delle

tendenze più peculiari osservate negli ultimi anni nel comportamento delle organizzazioni criminali: l'impiego dei cc.dd. *criptofonini*, ovvero della tecnologia crittografica applicata alle comunicazioni telefoniche. Attesa la vastità e la portata del fenomeno, testimoniata da numerose altre OTF (*Operational Task Force*) coordinate da Europol[3], nel presente contributo si vogliono esplorare, da un lato, le caratteristiche tecniche che rendono tali device così desiderabili da parte di OCG (*Organized Crime Groups*) sparsi in tutto il mondo e, dall'altro, i limiti all'utilizzo in sede procedimentale dei dati e delle informazioni scambiate mediante il ricorso a tali strumentazioni, analizzando l'interessante contenuto della recente Sentenza n. 6364/2023 del 15 febbraio 2023 della Suprema Corte di Cassazione.

2. Cosa sono i criptofonini

I *criptofonini* sono device prodotti da società – tra cui, le più note, sono *SKY Ecc* ed *Encrochat* – specializzate nell'erogazione di servizi di telecomunicazione capaci di consentire la criptazione del contenuto delle comunicazioni. Si tratta, in particolare, di smartphone opportunamente modificati nel *software* (prevalentemente il sistema *Android* o *Blackberry*), con l'unico scopo di garantirne l'inviolabilità da parte di "terzi". Nello specifico, il sistema operativo di tali dispositivi è dotato di peculiari requisiti di sicurezza che si possono riassumere nella:
- cifratura dei dati trasmessi e di quelli memorizzati;
- possibilità per l'utilizzatore di cancellare, quasi in tempo reale e anche da remoto, l'intera memoria del telefono inserendo un cd. *panic code*;
- possibilità di segnalare la presenza di sistemi di individuazione (c.d. *Imsi Catcher*) o di tentativi di aggressione informatica da parte di agenti esterni;

In dettaglio, tali sistemi di comunicazione non sono basati sulla tecnologia c.d. *pin to pin* (tipo *Blackberry*, cioè su un sistema crittografico dove le chiavi di cifratura sono collocate in un *server*), bensì sul sistema c.d. *end to end*, che prevede la cifratura delle conversazioni mediante l'utilizzo di chiavi depositate *esclusivamente* sui dispositivi che colloquiano fra loro. La principale conseguenza di tale configurazione è che neanche il gestore del servizio è in grado di conoscere le chiavi utilizzate e, di conseguenza, il contenuto delle comunicazioni.

3. I principi espressi dalla Cassazione

Chiamata ad esprimersi sull'utilizzo in sede giudiziaria di dati scambiati su piattaforma *Encrochat*, acquisiti da una Squadra Investigativa Comune (S.I.C.)[4] franco-belga-olandese coordinata da *Europol*, ed "*introdotti*" in un procedimento penale italiano mediante un Ordine Europeo di Indagine (O.E.I.)[5], nella predetta sentenza, la Suprema Corte ha sancito – tra l'altro – due importanti principi riguardanti, rispettivamente, la natura giuridica delle *chat* captate e la valutazione circa la loro legittima modalità di acquisizione.

3.a. La natura delle *chat*

Con riguardo al primo punto, inerente alla natura giuridica delle *chat*, occorre *in limine* distinguere due diversi tipi di operazione che gli organi investigativi possono effettuare nello svolgimento delle indagini di polizia giudiziaria:
- operazioni di captazione e di r*egistrazione del messaggio cifrato*, nel momento in cui lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, con la possibilità che i dati peraltro possano transitare anche attraverso server ubicati in Stati diversi da quelli nei quali si trovano fisicamente i soggetti che stanno comunicando tra loro;
- *operazioni di decriptazione del contenuto del messaggio*, necessarie per trasformare mere stringhe informatiche in dati comunicativi intellegibili, solitamente resa possibile dalla "chiave" di decriptazione fornita dal *service provider*, che la sfrutta a fini commerciali.

Ebbene, pare pacifico come solo alla prima delle due operazioni faccia riferimento all'art. 266-*bis* c.p.p., che – come noto – estende l'applicabilità delle norme del codice di rito relative alle ordinarie intercettazioni di conversazioni o comunicazioni tra soggetti a distanza, alle intercettazioni di flussi di comunicazioni relativi a "*sistemi telematici ovvero intercorrenti tra più sistemi telematici*", ossia flussi che non avvengono "*in via diretta*" tra apparecchi informatici, ma che sfruttano la trasmissione dei dati "*in via telematica*" (*i.e*. via cavo, ponti radio o per mezzo di altra analoga strumentazione tecnica)[6].

Difatti, qualora il messaggio telematico sia "*in chiaro*", cioè non criptato, la sua captazione e la sua registrazione ne rendono immediatamente intellegibile il contenuto e, di conseguenza, direttamente utilizzabile a fini di prova il relativo risultato conoscitivo.
Nel caso di specie, al contrario, la Suprema Corte ha precisato che deve escludersi che l'attività di acquisizione e di decifrazione di tali dati comunicativi rientri nel novero delle attività di intercettazione, dal momento che queste ultime postulano la captazione di un "*flusso di comunicazioni in atto*". Nel caso in esame, trova infatti applicazione il diverso art. 234-bis c.p.p.[7], che prevede che «*È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare* (ovvero – nel caso dei dati custoditi nei *criptofonini* – il s*ervice provider* detentore della chiave di decriptazione, n.d.r.)».

Come evidenziato dal giudice di nomofilachia, tale ultima disposizione trova difatti pacifica applicazione nel caso in esame dal momento che l'acquisizione dei dati ha riguardato non un documento cartaceo o analogico, bensì un documento inteso come «*rappresentazione comunicativa incorporata in una base materiale con un metodo digitale*», ovverosia dati in-

formatici che hanno consentito di rendere intellegibile il contenuto di stringhe redatte secondo il linguaggio informatico.

3.b. L'acquisizione delle *chat*

Con riguardo al secondo aspetto di interesse operativo, ovvero l'impiego nel corso delle indagini preliminari di dati decriptati rinvenienti dai canali della cooperazione europea giudiziaria e di polizia, rifacendosi ad un consolidato orientamento in materia di rogatoria attiva, il giudice di legittimità ha sostenuto che – in tali casi – l'utilizzazione degli atti non è condizionata ad un preliminare (*rectius*: pregiudiziale) accertamento da parte del giudice italiano volto alla verifica di regolarità delle modalità di acquisizione utilizzate dall'autorità straniera.

Alla radice di tale orientamento, in particolare, vige una "*presunzione di legittimità dell'attività svolta* (*aliunde*, n.d.r.)", ovvero – secondo il disposto della Cassazione – il "*principio della reciproca fiducia in ordine alla regolarità dell'attività investigativa svolta e dell'assenza di specifiche deduzioni in punto di violazione dei principi generali dell'ordinamento interno*". Il corollario operativo e procedurale che se ne trae è, dunque, che spetta unicamente al giudice straniero la verifica della correttezza della procedura seguita per l'acquisizione del dato, nonché l'eventuale risoluzione di ogni altra questione relativa alle irregolarità lamentate nella fase delle indagini preliminari.
Tale assunto appare, inoltre, ancora più solido nel caso in esame, che peraltro ha ad oggetto non una richiesta di procedere a intercettazioni da parte dell'Autorità giudiziaria italiana, ma di una richiesta di acquisizione degli esiti documentali di attività d'indagine che l'autorità straniera ha già svolto, nella sua piena autonomia, nel rispetto della sua legislazione in relazione ad altri reati.

4. Il "*guscio*" tecnologico delle organizzazioni criminali

Lo studio e l'osservazione dell'impiego delle nuove tecnologie da parte delle organizzazioni criminali costituisce una sfida professionale decisiva per la polizia giudiziaria, da sempre chiamata ad uno sforzo di aggiornamento tempestivo dei propri sistemi di prevenzione e repressione dei reati, specie se commessi in forma associativa e su scala transnazionale.
In questa prospettiva, la penetrazione del "*guscio*" tecnologico dentro il quale agiscono le organizzazioni malavitose, può rivelarsi un vero e proprio catalizzatore investigativo grazie ai dati ed alle informazioni che ne possono derivare, come ha plasticamente dimostrato l'operazione TROJAN SHIELD/GREENLIGHT, coordinata da Europol. Una miniera di dati grezzi che, tuttavia, necessitano di essere manipolati con i sofisticati strumenti del diritto, per potersi tramutare in *elementi di prova*.

Capitano Guardia di Finanza

1 - I risultati dell'indagine sono consuntivati nel press release dell'agenzia EUROPOL, dell'8 giugno 2021, reperibile sul sito *europol.europa.eu* (sezione media-press).
2 - Al momento delle operazioni, la piattaforma era cresciuta fino a servire più di 12 mila dispositivi criptati di oltre 300 organizzazioni criminali, operanti in oltre 100 paesi. Tra gli *user* comparivano esponenti della criminalità organizzata italiana, bande di motociclisti fuorilegge e organizzazioni internazionali di traffico di droga.
3 - Tra le indagini più rappresentative: operazione 26SASSENHEIM, che ha consentito alle Autorità olandesi l'acquisizione e la decodifica di circa 3 milioni di comunicazioni effettuate dal 2015 al 2018, con i apparati Black Berry PGP, contenuti in alcuni server ubicati in Costa Rica e Canada; operazione EMMA 95/LEMONT 26: relativa all'attività di una Squadra Investigativa Comune, costituita nel 2020 tra Francia e Olanda, contro la piattaforma Encrochat; operazione LIMIT relativa all'attività di una OTF, costituita nel 2021, dalle Autorità di Belgio, Francia e Olanda, con il sostegno di Europol ed Eurojust, contro la piattaforma Sky Ecc.
4 - D.Lgs. 15 febbraio 2016, n. 34, ha recepito la Decisione quadro n. 2002/465/GAI del Consiglio del 13 giugno 2002.
5 - Di cui alla Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014, concernente l'Ordine Europeo di Indagine Penale (O.E.I.), recepita in Italia con il D.Lgs. 21 giugno 2017, n. 108.
6 - Nel senso della qualificazione come intercettazione ai sensi dell'art. 266-bis cod. proc. pen. dell'acquisizione dei contenuti di messaggistica in atto effettuata con sistema *Blackberry*, cfr. Cassazioni n. 49896 del 15 ottobre 2019; n. 47557 del 26 settembre 2019 e n. 50452 del 10 novembre 2015.
7 - Introdotto dall'art. 2, comma 1-bis, del decreto legge 18 febbraio 2015, n. 7, convertito dalla legge 17 aprile 2015, n. 43.