Poliziamoderna

Piattaforme criptate e prova penale

1. Premessa Ad oggi, le indagini penali sulle piattaforme criptate rappresentano una delle principali sfide che l'*environment law enforcement* si trova ad affrontare, ma da domani alle difficoltà di ordine tecnico – legate al fatto che si tratta di piattaforme dotate di importanti gradi di crittografia, con *server* spesso allocati in diversi Paesi del mondo – si affiancheranno criticità di natura giuridica in rapporto al corretto inquadramento delle attività espletate e alla conseguente diagnosi di utilizzabilità processuale dei dati raccolti. L'obiettivo dell'analisi è verificare la compatibilità delle investigazioni esperite sulle piattaforme criptate con le categorie probatorie già esistenti, al fine di accertare l'esistenza di una odierna copertura normativa idonea a garantire la tenuta costituzionale e codicistica degli elementi di prova acquisiti.

2. La nuova frontiere dell'etere digitale Si dice ormai da tanto che la rivoluzione informatica dell'ultimo tempo ha profondamente alterato le abitudini degli individui, incidendo sul modo di vivere, comunicare, interagire e intendere le relazioni interpersonali; di conseguenza, anche le modalità di concretizzazione delle più o meno tradizionali *species* delittuose sono mutate, plasmandosi in ragione di un rinnovato contesto sociale, politico ed economico.

Allo stesso tempo, sotto un profilo propriamente processuale, da anni si registra un frenetico ricorso a nuovi strumenti di indagine tecnologici che risultano indispensabili a rendere effettiva la lotta contro le più evolute forme di criminalità. Progredendo, infatti, con straordinaria velocità tanto le tecnologie di captazione – che diventano sofisticate ed invasive - quanto le modalità di elusione delle captazioni – che si affidano all'adozione di sistemi di criptazione dei messaggi scambiati -, risulta imprescindibile ricorrere a nuovi strumenti investigativi ad alto potenziale tecnico per penetrare canali criminali di comunicazione o scambio di informazioni utilizzati per la commissione di reati di particolare allarme sociale.

A tali cambiamenti in chiave progressista, il giurista sembra oramai abituato, sperimentando l'uso del captatore informatico e, poi, quello dell'*Imsi catcher*. Si pensava ingenuamente che il ritmo incalzante del progresso scientifico si fosse arrestato e, invece, a distanza di pochi anni dalla tipizzazione normativa del *virus* informatico, la questione relativa all'impiego di nuove metodologie di indagine si impone con tutta la sua dirompenza. L'ultima frontiera delle investigazioni è rappresentata dalle attività esperite sulle piattaforme di comunicazioni criptate, di recente utilizzate anche dalle organizzazioni criminali per condurre e pianificare i propri traffici illeciti. Questa volta non è lo strumento con cui l'investigazione viene esperita ad essere innovato ma la tecnica utilizzata per acquisire informazioni utili al processo: se in passato l'investigazione risultava circoscritta a specifici "ambienti" (come nel

caso delle microspie) o a determinate aree di interesse (come nel caso del *virus Trojan)*, allo stato è l'etere digitale il nuovo spazio da "esplorare", cioè il *server* sul quale transitano tutti i flussi informativi degli utenti che utilizzano servizi di comunicazioni criptati*.* Di conseguenza, cambiando lo spazio nel quale gli investigatori possono recuperare elementi di prova, cambiano anche le modalità con cui le indagini devono essere esperite.

Già da una prima analisi, emerge che quelle sulle *encrypted platforms* sono investigazioni assai complesse sia sotto il profilo operativo che giuridico. Da una parte, si tratta di indagare su piattaforme dotate di importanti gradi di crittografia con *server* spesso allocati in diverse parti del mondo, sfruttando le potenzialità offerte dai cosiddetti *big data*; in questi casi, inevitabilmente, le forze di polizia necessitano della stretta collaborazione degli organi inquirenti di Stati diversi da quello in cui la necessità investigativa ha avuto origine. Dall'altra, si profilano criticità di natura classificatoria, determinate dalla difficoltà di individuare la categoria probatoria in cui ascrivere le attività espletate su tali sistemi e, di conseguenza, emergono criticità relative alla diagnosi di utilizzabilità processuale dei dati ottenuti a seguito di decriptazione dei dati giacenti sui *server.* Va, inoltre, precisato che in materia, il *law enforcement* nazionale è in netto ritardo rispetto agli altri Paesi europei, perché, ad oggi, l'Italia ha svolto un ruolo di "osservatore passivo" rispetto alle attività condotte da altri Paesi, posto che le forze di polizia italiane hanno ricevuto pacchetti di dati da analizzare ed eventualmente utilizzare secondo modalità definite da altri ma non hanno svolto alcuna attività investigativa autonoma sui *server* criptati che, peraltro, (almeno allo stato) non sono mai risultati allocati sul territorio nazionale. Non è, però, inverosimile immaginare che di qui a qualche tempo le autorità nazionali si troveranno a ricoprire il ruolo di attori nelle investigazioni sulle piattaforme criptate.

Occorre interrogarsi sin d'ora circa la possibilità di svolgere "in prima persona" tali attività di indagine su *server* ubicati all'estero e/o in territorio nazionale.

In quest'ottica, il giurista è chiamato a comprendere se e in che termini le indagini sulle *encrypted communication platforms* possano trovare impiego nel processo penale, individuando la corretta cornice giuridica nella quale le attività possono essere sussunte.

3. Criptofonini e *encrypted communication platforms* In tema di investigazioni tecnico-scientifiche, nessuna considerazione giuridica può prescindere dall'analisi del dato informatico, ossia dal confronto con le caratteristiche ontologiche dei prodotti della tecnologia quale prodromo essenziale per cogliere al meglio le riflessioni giuridiche che verranno svolte nel prosieguo; in questo senso, solo un preliminare vaglio circa il funzionamento dei criptofonini rende possibile l'individuazione delle problematiche che sottendono le indagini sulle piattaforme criptate e il conseguente impiego nel processo penale.

Un *cryptophone* – anche definito *Dedicated encrypted communication device* (Decd) – è un tipo di *smartphone* specificamente progettato per fornire comunicazioni sicure e proteggere da *hacking* e sorveglianza.

Inoltre, tali *devices* si servono delle *Hardened secure communication platforms* (Hscp), più comunemente definite piattaforme di comunicazioni criptate, ossia di sistemi operativi e applicazioni installate su dispositivi di comunicazione sicuri e protetti fisicamente. Le più note sono *EncroChat* e *Sky ECC*, anche se in commercio ne esistono numerose e con differenti caratteristiche.

Sotto il profilo strettamente tecnico, i criptofonini si servono di applicazioni e servizi dedicati che garantiscono l'inaccessibilità al sistema e la sicurezza dei dati *ivi* contenuti. Tra questi vanno ricordati:

a) *Zero-attack surface*. Tutti i punti di ingresso dei moderni dispositivi mobili – quali servizi Google, servizi Gsm, Sms, *Bluetooth*, Nfc, Gps, porta Usb abilitata alla sola ricarica – vengono disabilitati.

b) *Trusted updates*. Gli aggiornamenti vengono emessi e firmati digitalmente esclusivamente attraverso il *Secure administration system* (Sas): i dispositivi applicano gli aggiornamenti solo dopo aver verificato l'autenticità della firma digitale.

c) *Multiple password protection*. L'archiviazione, il sistema operativo e le applicazioni sicure del dispositivo sono tutti protetti da *passphrase* separate, ciascuna impostata per attivare una procedura di cancellazione in caso di errore per un numero consecutivo di volte.

d) *Multiple levels of encryption*. Le comunicazioni in entrata e in uscita sono crittografate *end-to-end* e trasmesse su una Rete crittografata (Vpn). La configurazione Vpn è dinamica e può essere modificata da remoto dagli amministratori. Anche tutti i dati memorizzati sul dispositivo sono crittografati.

e) *Encrypted VoIP*. Alcuni criptofonini consentono all'utente di camuffare la propria voce con una serie di *vocoder* digitali preconfigurati, tra cui: *robot* e generiche voci maschili e femminili.

f) *Volatile data*. I dati possono essere distrutti: grazie a una cancellazione remota eseguita dal rivenditore per il tramite del *software Mobile device management* attivando una procedura tramite digitazione di un codice "antipanico" (c.d. *panic* o *Sos code*), per il cui tramite il dispositivo invia un messaggio automatico ai contatti di emergenza dell'utente.

g) *Data dissimulation*. Utilizzo di funzionalità anti-tracciamento, come Imei, Imsi e *App* falsi per fuorviare i controlli di polizia.

h) *Imsi catcher detector*. Rileva ed evita la stazione base falsa nelle reti Gsm/Umts.

Sotto il profilo operativo, gli investigatori – non potendo interferire direttamente nella comunicazione poiché dotata di imponenti e pressoché invalicabili gradi di crittografia – hanno bisogno di "intromettersi" direttamente sul *server* per acquisire le informazioni utili alle indagini.

In questo contesto, si prospettano due possibilità investigative: procedere al *takedown*, ossia all'apprensione in blocco di tutti i dati giacenti sulla piattaforma attraverso il "congelamento" del *server*, oppure, penetrando la stessa, captare *live* il flusso di comunicazioni in transito.

4. Le inedite decisioni di legittimità La giurisprudenza, sul punto, si è già espressa. Come sempre accade quando si ha a che fare con strumenti di indagine inediti ad alto potenziale tecnologico, sono i giudici di legittimità – prima ancora del legislatore – ad intervenire per delineare i limiti e le condizioni di impiego dei risultati investigativi in sede processuale, molto spesso a seguito delle sollecitazioni provenienti dalle Corti sovranazionali e/o dalle Corti di altri Paesi.

Non è un caso che, sulla scia di quanto sta accadendo in altri Stati europei, la questione relativa all'utilizzabilità dei dati acquisiti sui *criptophones* venga affrontata a più riprese dalla Suprema Corte con l'intento di delineare uno "statuto" delle investigazioni sulle piattaforme di comunicazione criptate.

Prima ancora di analizzare il contenuto delle pronunce che si susseguono freneticamente, occorre soffermarsi brevemente sul caso di specie da cui traggono origine le diverse decisioni in materia.

Pur non esse

...

04/09/2023