Senato della Repubblica XIX LEGISLATURA

Giunte e Commissioni

RESOCONTO STENOGRAFICO n. 18

N.B. I resoconti stenografici delle sedute di ciascuna indagine conoscitiva seguono una numerazione indipendente.

2ª COMMISSIONE PERMANENTE (Giustizia)

INDAGINE CONOSCITIVA SUL TEMA DELLE INTERCETTAZIONI

56ª seduta: martedì 20 giugno 2023

Presidenza del presidente BONGIORNO

INDICE

Audizione del Comandante del Raggruppamento operativo speciale dei Carabinieri.

PRESIDENTE . . . . . *Pag.* 3, 5, 6 e *passim* | * *ANGELOSANTO* . . . . . *Pag.* 3, 5, 7

N.B. L'asterisco accanto al nome riportato nell'indice della seduta indica che gli interventi sono stati rivisti dagli oratori

Sigle dei Gruppi parlamentari: Azione-Italia Viva-RenewEurope: Az-IV-RE; Civici d'Italia-Noi Moderati (UDC-Coraggio Italia-Noi con l'Italia-Italia al Centro)-MAIE: Cd'I-NM (UDC-CI-NcI-IaC)-MAIE; Forza Italia-Berlusconi Presidente-PPE: FI-BP-PPE; Fratelli d'Italia: FdI; Lega Salvini Premier-Partito Sardo d'Azione: LSP-PSd'Az; MoVimento 5 Stelle: M5S; Partito Democratico-Italia Democratica e Progressista: PD-IDP; Per le Autonomie (SVP-Patt, Campobase, Sud Chiama Nord): Aut (SVP-Patt, Cb, SCN); Misto: Misto; Misto-ALLEANZA VERDI E SINISTRA: Misto-AVS.

Interviene, ai sensi dell'articolo 48 del Regolamento, il generale di divisione Pasquale Angelosanto, Comandante del Raggruppamento Operativo Speciale dei Carabinieri, accompagnato dal colonnello Leandro Piccoli, Comandante del III Reparto Analisi del ROS.

I lavori hanno inizio alle ore 9,30.

SULLA PUBBLICITÀ DEI LAVORI

PRESIDENTE. Avverto che, previa autorizzazione del Presidente del Senato, la pubblicità della seduta odierna è assicurata attraverso il resoconto stenografico.

PROCEDURE INFORMATIVE

Audizione del Comandante del Raggruppamento operativo speciale dei Carabinieri.

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sul tema delle intercettazioni, sospesa nella seduta del 27 aprile.

È oggi prevista l'audizione del comandante del Raggruppamento operativo speciale (ROS) dei Carabinieri, generale di divisione Pasquale Angelosanto, che ringrazio. Avverto il nostro audito che, per rendere omogeneo il tempo concesso a tutti gli auditi, è prevista un'introduzione da parte sua, che si deve contenere nell'ambito di otto o dieci minuti, a cui poi seguiranno le eventuali domande da parte dei commissari e infine avrà a disposizione altri otto o dieci minuti per le conclusioni.

Cedo pertanto la parola al generale Angelosanto.

ANGELOSANTO. Signor Presidente, onorevoli senatrici e senatori, vi ringrazio dell'opportunità odierna. Ho preparato un testo scritto, che consegno all'Ufficio di Presidenza e che è articolato in diversi capitoli. Per ben inquadrare il tema delle intercettazioni, ho ritenuto necessario parlare innanzitutto delle forme di minaccia che ci troviamo ad affrontare. Ci occupiamo infatti della minaccia derivante dalla criminalità mafiosa, dalla criminalità organizzata e, in genere, dalle organizzazioni più strutturate, come quelle dedite al traffico internazionale degli stupefacenti o le organizzazioni straniere di matrice etnica. A ciò si aggiunge la minaccia del terrorismo internazionale di matrice confessionale e di quello interno, declinato nelle espressioni dell'anarchia insurrezionalista, dell'estrema destra e della sinistra marxista-leninista. Ho ritenuto di dover fare questa premessa perché, in estrema sintesi, le organizzazioni criminali ricorrono

agli strumenti tecnologici per assicurare le comunicazioni necessarie alla loro stessa sopravvivenza e allo svolgimento delle loro attività illecite.

Affronterò poi il tema delle intercettazioni, focalizzando l'attenzione in particolar modo sulle piattaforme di comunicazione crittografata, che sono oggi il vero problema investigativo che ci troviamo ad affrontare e che stiamo affrontando già da qualche anno, d'intesa con l'autorità giudiziaria, soprattutto nell'ambito della cooperazione internazionale di polizia e giudiziaria. Ci sono poi le indagini nel *web*, soprattutto quelle che si possono svolgere attraverso il monitoraggio della rete nel cosiddetto *dark web*, che è la parte più profonda e più nascosta del *web*, dove avvengono scambi di natura illecita. Ci sono poi gli *spyware*, ovvero i captatori telematici. Ho inoltre ritenuto di affrontare anche il tema del *data retention*, perché si tratta di un problema tecnico che, ogni volta che affrontiamo un'indagine, ci troviamo a dover superare. Ho anche ritenuto di fare un breve cenno alle intercettazioni preventive e a quelli che, secondo noi, sono i quadri esigenziali, che indicano cioè cosa dovremmo avere, squisitamente sotto il profilo del potenziamento tecnologico o delle risorse umane. Per alcuni di questi singoli argomenti ho anche indicato quali potrebbero essere le soluzioni normative, per agevolare il compito degli organi incaricati di svolgere le attività di indagine.

La prima parte del documento riguarda l'assetto del Raggruppamento. Ho citato inizialmente queste due forme di minaccia, perché il raggruppamento operativo speciale – si tratta di una peculiarità del ROS rispetto agli altri servizi centrali – è deputato ad affrontarle entrambe, ovvero sia la criminalità mafiosa, sia quella terroristica ed eversiva. Dunque, per entrambe queste espressioni di minaccia il ROS segue le attività investigative che sono incardinate esclusivamente nell'ambito delle direzioni distrettuali antimafia e, quindi, in ambito distrettuale. Tali investigazioni sono svolte su delega delle procure della Repubblica.

Riguardo alla criminalità mafiosa, l'aspetto oggi qualificante – tralascio tutte le connotazioni che possono avere le forme di criminalità e le diverse mafie – è quello della transnazionalità delle organizzazioni e quindi il fatto che le organizzazioni – abbiamo la definizione normativa del delitto transnazionale e quindi siamo agevolati in questo – compiono reati o all'estero o esplicando le loro attività in più Stati. Detto questo, c'è un largo ricorso alle comunicazioni, come ho anticipato, soprattutto quelle criptofoniche, e all'utilizzo di sistemi tecnologici, anche per assicurare transazioni e pagamenti. Quindi, sotto questo aspetto, lo strumento delle intercettazioni si rivela fondamentale, non solo nel contrasto alle attività di tipo mafioso, ma anche per l'accertamento delle condotte strumentali all'esistenza e all'operatività dell'associazione stessa.

Per quanto riguarda invece la minaccia eversiva e terroristica, posso brevemente dire che c'è un ampio ricorso all'utilizzo del *web* da parte delle organizzazioni di matrice confessionale: faccio riferimento quindi ai due grandi *network* mondiali, cioè lo Stato Islamico e al-Qaeda. Ciò accade perché il *web* consente un'ampia diffusione di materiale propagandistico, di auto-apprendimento e di auto-istruzione, per la formazione dei

singoli combattenti. Questo è un aspetto di fondamentale importanza, per contrastare le modalità di aggressione di tali formazioni terroristiche internazionali. La minaccia maggiore è infatti costituita dagli attori solitari, i cosiddetti *lone actors*, che vanno incontro ad una auto-radicalizzazione che spesso avviene attraverso la rete. C'è quindi questa formazione da parte di coloro che intendono aderire all'uno o all'altro tipo di ideologia per cui il *web* diventa fondamentale. Oltre al *web*, c'è un ampio ricorso, anche per questo aspetto, ai *social network* che costituiscono un moltiplicatore dell'ideologia estremista e consentono la diffusione delle cosiddette narrative istigatorie. Pertanto, anche in questo caso c'è un ampio ricorso al *web*. Da ciò deriva l'importanza delle intercettazioni telematiche e di altri tipi di intercettazioni o di monitoraggio del *web*.

Lo stesso vale anche per quanto riguarda le ideologie estremiste della destra suprematista o accelerazionista. C'è dunque un'ampia diffusione nel *web* di propaganda estremista di carattere xenofobo, neonazista e suprematista, in grado di far presa sui soggetti di giovane età e anche in questo caso c'è un ricorso ai *social network*. Quindi, anche questo aspetto è importante perché i processi di radicalizzazione che avvengono nell'ambito dell'ideologia estremista di matrice confessionale hanno delle analogie con i processi di radicalizzazione degli estremisti di destra, per cui il *web* diventa ancora una volta centrale.

Riguardo invece alla minaccia anarco-insurrezionalista c'è un ricorso al *web* per quanto riguarda tutto l'aspetto che definiamo di controinformazione e quindi di illustrazione dell'ideologia e di lettura della realtà, con la diffusione di documenti relativi alle campagne di lotta, che precedono l'attività delittuosa, o anche con le rivendicazioni che avvengono attraverso il *web*.

PRESIDENTE. Generale, la interrompo un momento e poi le ridò subito la parola.

Per ragioni organizzative, come sapete, dobbiamo attenerci ai tempi. Siccome siamo a metà dell'intervento, se nessuno intende porre quesiti, io chiederei se nella seconda parte del suo intervento si può soffermare (avendo a disposizione soltanto gli ultimi 8-10 minuti) in particolare sui temi ai quali faceva cenno prima quando leggeva l'indice, cioè quelli inerenti le problematiche tecnologiche connesse a queste piattaforme crittografate oppure ai *trojan,* insomma sulla parte più tecnologica.

ANGELOSANTO. Va bene. A questo punto salterò tutto l'aspetto che riguarda le attività d'intercettazione e le procedure seguite perché fanno riferimento alla legge.

PRESIDENTE. Comunque noi abbiamo il suo testo.

ANGELOSANTO. Sì, nel testo ci sono aspetti importanti che noi abbiamo desunto e che seguiamo nell'effettuazione dell'attività d'intercettazione e che fanno riferimento alle circolari diffuse dalle procure distret-

tuali della Repubblica. In questo caso ho preso ad esempio quattro grandi procure (quelle di Milano, Roma, Reggio Calabria e Palermo) con le indicazioni che sono state date dai procuratori per quanto riguarda le trascrizioni delle conversazioni, soprattutto in riferimento a quelle rilevanti o alla non trascrizione delle intercettazioni irrilevanti ai fini dell'indagine o inutilizzabili.

È stato anche affrontato il tema della remotizzazione, che per noi è importantissima, e se vuole posso tornare su questo argomento.

Le piattaforme di comunicazione crittografata sono sistemi in grado di garantire le comunicazioni eludendo completamente le investigazioni, cioè la comunicazione che avviene attraverso le utenze crittografate non possono essere intercettate. Oggi non siamo in grado di poterle intercettare, benché si siano fatti dei grossi passi avanti nell'ambito della cooperazione, perché alcune polizie europee sono state in grado di acquisire le cosiddette *chat* tra telefoni criptati e questo ci ha consentito una lettura successiva delle *chat*.

I criptofonini sono telefoni dedicati che consentono la comunicazione vocale e di messaggistica in forma cifrata. Si tratta di sistemi privi della funzionalità telefonica tradizionale; per esempio, vengono utilizzate delle *Subscriber identity module* (SIM) soprattutto straniere, quindi acquistate all'estero, e abilitate solo al traffico dati, quindi non c'è la comunicazione telefonica, oppure per esempio non hanno i sistemi di localizzazione GPS come hanno i nostri *smartphone,* per cui non sono intercettabili né geolocalizzabili, due aspetti fondamentali nell'attività d'indagine.

La cifratura, quindi, avviene sia sulla trasmissione dei dati, sia sui contenuti dello stesso apparecchio telefonico, per cui anche il suo contenuto è cifrato. Ciò significa che i dati memorizzati sui dispositivi possono essere cancellati in qualsiasi momento, ma soprattutto sfuggono agli accertamenti fatti nella cosiddetta attività forense, quindi alla duplicazione dei contenuti dei telefonini per poterli esaminare. La copia forense del dispositivo può cioè portare a un nulla di fatto; non si riesce a farla, perché comunque anche in questo caso i dati non sono intelligibili, sia quelli delle intercettazioni sia quelli memorizzati.

Di per sé il telefono criptato non è uno strumento illegale; è un telefono che viene venduto perché consente la comunicazione rispettando la *privacy* dell'utente ed è in commercio; ciò che lo rende uno strumento illecito sono le modalità di commercializzazione, perché non si trova al pubblico mercato; in genere, è acquistato all'interno di piattaforme *web* conosciute solo da chi ha la volontà di acquistare questo tipo di telefonia e il pagamento avviene con criptovalute o comunque su canali bancari sicuri; queste modalità già fanno intendere in premessa che non siamo di fronte a uno strumento che viene acquistato per l'utilizzo lecito.

PRESIDENTE. Il fatto che non si riescono a intercettare dipende da limiti della tecnologia che non ci riesce o anche da un tema normativo che in qualche modo preclude qualcosa su questi telefonini.

ANGELOSANTO. Ci sono entrambe le ragioni: c'è un problema tecnico, perché i *server* sui quali risiedono le piattaforme di gestione di questi criptotelefoni (ce ne sono tantissime, noi ne abbiamo individuate molte) sono dislocati all'estero e per poter effettuare un'intercettazione bisognerebbe entrare nel *server.* Le polizie straniere con le quali abbiamo collaborato, che però ci forniscono una documentazione soltanto a comunicazione avvenuta (quindi noi non abbiamo la possibilità di effettuare l'intercettazione cosiddetta *live,* mentre avviene la comunicazione), hanno ottenuto questi dati con un hackeraggio legale, intervenendo sul *server,* autorizzati dalle magistrature dello Stato dove operano le Forze di polizia. Questo tipo di acquisizione dei dati ha consentito alle forze di polizia di mettere a disposizione delle polizie degli altri Stati i dati relativi alle comunicazioni, attraverso la riconducibilità alle utenze e all'operatività sul territorio nazionale.

A questo punto, però, sorge un altro problema e cioè quello dell'utilizzabilità di queste comunicazioni, tant'è che c'è una giurisprudenza di merito e di legittimità che assimila i dati relativi alle *chat* ai documenti, quindi alla prova documentale (articolo 234 del codice di procedura penale). Sono pertanto considerati dati di documenti informatici e con questo inquadramento noi siamo riusciti ad avere, per esempio, le *chat* del sistema EncroChat, di Sky ECC o anche di altri gestori.

Consideri che il problema è normativo per l'utilizzabilità, ma è problematico per quanto riguarda la nostra capacità di poter effettuare intercettazioni, perché l'intercettazione della criptofonia non sarebbe puntata sul bersaglio, ma sarebbe un'intercettazione aperta e ciò determina una enorme difficoltà di carattere normativo e tecnico.

PRESIDENTE. Come il *trojan*.

ANGELOSANTO. Sì, nel senso che quando il *trojan* effettua intercettazioni in un ambiente intercetta tutti quelli che vi transitano, ma ci sono limitazioni nella fase operativa o meglio la polizia giudiziaria che opera è obbligata a monitorare l'ambiente.

Detto ciò, c'è questa difficoltà perché non abbiamo una copertura giuridica per l'accesso ai *server* delle piattaforme criptate, per cui non c'è norma che ci consenta di fare questo lavoro.

Rispetto alle diverse possibilità esistenti, io mi sono permesso di far riferimento alla normativa francese, che ha individuato nell'utilizzo dei sistemi di criptofonia non registrati una forma di agevolazione delle condotte criminali, ritenendola essa stessa una condotta criminale; è pertanto prevista l'illiceità della condotta di erogazione di queste prestazioni di criptofonia, se non sono accompagnate da dichiarazioni conformi alle autorità preposte. Il gestore di telefonia dovrebbe cioè dichiarare l'utilizzo della sua rete, perché comunque i criptofonini si appoggiano in *roaming* alla rete nazionale, per cui ad esempio il criptotelefonino della piattaforma EncroChat o di Sky ECC di società olandese o statunitense che opera in Italia si appoggia alle reti di telefonia italiane, ma le nostre reti

di telefonia italiane non sono in grado di poterlo dire perché l'utilizzatore del telefonino è coperto dall'anonimato che è previsto dalla legislazione del Paese nel quale immatricola il telefonino o l'utenza. Pertanto, essendo garantita l'anonimizzazione a monte, anche l'intervento sul gestore di telefonia italiano non porterebbe all'identificazione.

Noi ci arriviamo attraverso un'operazione complicatissima di attività investigativa, cioè attraverso il pedinamento, nel momento in cui ci accorgiamo, per esempio, che un pedinato utilizza un telefono che non risulta tra quelli intercettati, per cui assistiamo ad una comunicazione telefonica oppure facciamo una intercettazione ambientale, ad esempio in un'autovettura o in un'abitazione, grazie alla quale registriamo in sonoro una comunicazione telefonica che avviene su un canale non controllato. Facciamo quindi riferimento al gestore e alle celle che coprono l'area e al momento in cui abbiamo constatato questo utilizzo per individuare il telefono che in quel momento si è appoggiato alla rete telefonica e al gestore – Tim, Vodafone e così via – al quale chiediamo i dati perché il gestore, ai fini commerciali, registra il *roaming*. In tal modo riusciamo ad apprendere che si tratta, magari, di un'utenza di un gestore americano che ha un certo numero, un certo indirizzo di rete e così via. Quindi, attraverso questa operazione riusciamo ad individuarlo, però, se non c'è questa attività, il telefono sfugge al controllo.

Un'altra possibilità è quella di chiedere comunque ai gestori di telefonia italiani, e quindi a chi è obbligato a fornire le prestazioni, di chiedere la registrazione e di non accogliere i telefonini criptati che non sono registrati o quantomeno i cui utenti non sono identificati. Questa potrebbe essere una soluzione normativa per cui il gestore di telefonia che assicuri il *roaming* anche del telefono criptato può farlo solo per la rete che consente l'individuazione del soggetto utilizzatore. Se non c'è questa possibilità, il gestore non dovrebbe assicurare il *roaming*. Questa potrebbe essere un'altra soluzione.

Una ulteriore soluzione, a proposito dell'hackeraggio legale di cui ho parlato, sarebbe quella di prevedere per utilizzare le operazioni speciali – e faccio riferimento all'articolo 9 della legge n. 146 del 2006 – determinati presupposti, cioè oltre a tutti i delitti indicati per le attività che scriminano la condotta, si dovrebbero inserire anche quelli che prevedono la commissione di delitti attraverso l'uso del telefono criptato. Questo ci consentirebbe di essere autorizzati a svolgere un'attività tecnica telematica di acquisizione del dato nel *server* di partenza. Questa potrebbe essere un'altra soluzione.

PRESIDENTE. Generale, purtroppo per motivi di tempo sono costretta ad interrompere questa interessante – almeno per me – audizione. Spero di trovare nei documenti che ci ha dato tutte le indicazioni per approfondire la tematica trattata.

Faccio presente che ho ricevuto soltanto adesso il documento, che sarà fotocopiato e messo a disposizione di tutti. Se ci può girare anche il *file*, potremmo inviarlo a tutti i commissari. Mi spiace davvero interrom-

perla su un argomento che stiamo studiando, ma alle ore 10 ci sarà una importante votazione in Aula.

La ringrazio e la saluto a nome di tutti i Commissari.

Dichiaro conclusa l'audizione odierna.

Rinvio il seguito dell'indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 9,55.

€ 1,00